
Installment 1 of 3: Cybersecurity and Physical Security

BY AUSTIN IGLEHEART

Introduction

The nation’s energy system is under threat from both cyber and physical attacks and is increasingly being targeted. The last two years have spurred state legislatures into action to improve the security of energy infrastructure within their state. The increasing number of cyberattacks directed at energy infrastructure owners and operators, like the high-profile Colonial Pipeline incident for example, has underscored the importance of proactively addressing cybersecurity threats to energy infrastructure. These attacks, together with physical threats like domestic terrorism, have influenced state legislators’ efforts to bolster the security of our nation’s energy infrastructure.

States generally have jurisdiction over “local” electric distribution. However, state statutes generally only grant state public utility commissions (PUCs) authority over investor-owned-utilities. Several states have extended PUC authority to certain aspects of municipal and cooperative utilities. Given that PUC authority is derived from state law, state legislatures are uniquely positioned to make a significant impact on the physical security and cybersecurity of their states’ energy infrastructure.

This is the first installment of NCSL’s Energy Security State Legislative Review, and outlines relevant legislation aimed at bolstering the security of states’ energy infrastructure against human threats between 2021 and 2022. Since the beginning of 2021, state legislatures have introduced nearly 500 bills broadly related to energy security. Of those, 99 measures were enacted or adopted by August 2022.
State legislatures considered at least 46 measures related to the cybersecurity of energy systems in 2021, a jump from 35 in 2020 but down from 50 in 2019. Of the measures introduced in 2021, over a dozen passed. In the past two legislative sessions, policymakers focused on emerging cyber threats (i.e., ransomware and threats from foreign adversaries) and on increasing their state’s ability and authority to respond to such threats and coordinate across agencies.

A renewed focus on cybersecurity has not replaced other security concerns, but builds on continued legislative efforts to protect the physical security of energy infrastructure. States across the country moved to create or enhance criminal and civil penalties for trespassing on or damaging energy infrastructure. Although not a new trend, the quantity of these physical security-related bills has increased over the last two years. While six states enacted legislation relating to physical security of energy infrastructure in 2020, 10 more states have considered legislation on the issue between 2021 and the first half of 2022. Federal agencies have issued several alerts about specific threats and potential attacks, such as domestic terrorism, and state legislators have responded to the threats by focusing on physical security.

Cybersecurity

Cyberattacks and similar threats to energy infrastructure can create significant economic and public safety risks, as demonstrated by recent attacks targeting both small and large energy providers.

In May 2021, the Colonial Pipeline Company was hit by a major ransomware attack that affected the pipeline’s digital systems; the hackers likely gained access through a compromised password. To prevent further spread of the malicious software, the company proactively shut down the pipeline, which runs from Texas to New York and supplies about half of the refined oil products for the East Coast. As the pipeline serves as a major energy conduit, the Biden administration deemed the attack a national security threat and declared an emergency. The same month, the Biden administration issued an executive order directing U.S. government agencies to take a series of proactive steps to bolster cybersecurity. The Transportation Security Administration has continued to take steps to improve the security of energy infrastructure, revising and reissuing cybersecurity requirements for oil and gas pipeline owners and operators in July 2022.
In November 2021, a Colorado utility serving about 35,000 customers was affected by a malicious cyberattack. The attack took many of its billing, processing, and other systems out of operation for more than a month, although there was no impact or disruption to their physical operations or service delivery. The breach highlights that malicious actors are targeting a range of energy infrastructure. Smaller utilities and infrastructure operators with limited resources to mitigate and recover quickly from attacks may benefit from state support and guidance to implement cybersecurity best practices.

The threat of government-sponsored cyberattacks on utility infrastructure has also become more apparent. The Federal Bureau of Investigation and U.S. Department of Homeland Security warned in February 2022 that the war in Ukraine could lead to attempted Russian attacks on U.S. critical infrastructure networks, including energy infrastructure. Russia exhibited this capability in late 2015 when they executed a coordinated, synchronized cyberattack that infected Ukrainian power companies’ systems with malware that caused power outages to over 200,000 customers across the country.

There is also the ongoing threat of supply chain compromise. In 2019 and 2020, the SolarWinds breach allowed hackers to gain access to the networks and systems of SolarWinds’ customers, which include various federal government agencies. The attack perpetrated by the Russian Foreign Intelligence Service raised U.S. policymakers’ awareness of the impact a comparable breach could have on America’s critical infrastructure. The federal government responded in December 2020 with an emergency mitigation directive for federal agencies whose software had been compromised and activated a coordination group within the executive branch.

State legislatures have taken major action to bolster the cybersecurity of their energy infrastructure amid new and increasing threats. Some measures have sought to increase energy cybersecurity investments from the public and private sector, including through PUC incentives and programs to leverage state and federal grants along with local funding. Several states are taking steps to create or expand state agency authorities to better deal with cyber threats. This could mean the creation of a new cybersecurity agency, or the expansion of existing authorities—namely disaster powers—to include cyber threats.

### STRENGTHENING PROTECTIONS AND PENALTIES FOR CYBER OFFENSES

<table>
<thead>
<tr>
<th>State</th>
<th>Bill Number</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska</td>
<td>HB 3</td>
<td>(enacted, 2022)</td>
<td>includes cyberattacks as well as a credible or imminent threat of a cyberattack in the state’s definition of disaster. This could help state authorities respond quickly to threats as they arise by allowing the governor to fully activate the state’s emergency response options and opening up state funding for repairs and emergency protective measures.</td>
</tr>
<tr>
<td>Illinois</td>
<td>HB 3523</td>
<td>(enacted, 2021)</td>
<td>included cyberattacks in the state’s definition of “disaster,” opening up disaster funding for responding to cyber threats.</td>
</tr>
<tr>
<td>Iowa</td>
<td>HB 2461</td>
<td>(failed, 2022)</td>
<td>would have defined the crime of ransomware and explicitly prohibited attempts to interrupt or impair the functioning of electricity and natural gas systems.</td>
</tr>
<tr>
<td>Maryland</td>
<td>HB 1339</td>
<td>(failed, 2022)</td>
<td>would have created a Critical Infrastructure Cybersecurity Grant Program to leverage funds from federal, state, and local grant programs for critical infrastructure cybersecurity improvements, and tasked the Department of Emergency Management with identifying funding. It also would have required certain cybersecurity practices and the development of regulations to protect the public from cyber threats.</td>
</tr>
</tbody>
</table>
**Tennessee** SB 2282 (enacted, 2022) requires utilities, including co-ops and municipally-owned utilities, to prepare and implement a cyber security plan to protect their facilities and related electronic data, and requires plans to be updated every two years to address new threats.

**Texas** SB 2116 (enacted, 2021) prohibits the state from contracting with certain foreign-owned companies for critical infrastructure projects—e.g. communication infrastructure, cybersecurity systems, electric grid projects, hazardous waste treatment systems, or water treatment facilities—in part due to cybersecurity concerns.

**Washington** HB 2044 (failed, 2022) would have expanded the state’s ransomware protection measures.

### CREATING NEW GOVERNMENT CYBERSECURITY AGENCIES AND AUTHORITIES

**Colorado** HB 1236 (enacted, 2021) augments the membership of the cybersecurity council and updates the state’s cyber operations center to better support state and federal information sharing following recent cyberattacks on both energy and transportation infrastructure in Colorado.

**Indiana** HB 1274 (failed, 2022) would have created a Volunteer Cyber Civilian Corps with experts that could help the Office of Technology with rapid response to cyberattacks.

**Massachusetts** SB 2088 (pending, 2021) would establish a cybersecurity control and review commission that includes one member with expertise in utility cybersecurity. Among other duties, the commission is tasked with developing utility sector-specific cybersecurity recommendations.

**Texas** HB 4196 (failed, 2021) would have required the PUC to develop and provide guidance on cybersecurity practices, and HB 4397 (failed, 2021) would have required additional monitoring around cybersecurity preparedness and implementation of training and best practices by utilities in the ERCOT power region.

**Utah** HB 280 (enacted, 2022) creates a new Cybersecurity Commission to identify and inform the governor of cyber threats and vulnerabilities towards Utah’s critical infrastructure, and analyze current cyber incident response capabilities and consequences in the event of a cyberattack.

### INFORMATION SHARING

States are focused on how to protect their energy infrastructure through data and information sharing between the private sector and government agencies responsible for threat prevention and response. Four states enacted new laws between 2021 and 2022 that require utilities to report on cyberattacks. One state has pursued a different approach, with policies that shield certain information about cybersecurity plans and threat responses from public disclosure to protect the security of public agencies, facilities, and related cybersecurity procedures and practices.
**Physical Infrastructure Security**

While states continue to discuss the cybersecurity of energy systems, legislatures are simultaneously addressing other pressing issues like physical infrastructure security. Physical infrastructure threats vary in source and complexity, from individual rifle attacks to domestic terrorism and threats from foreign adversaries. In February 2022, three people pleaded guilty to charges of plotting attacks on the U.S. power grid as part of a domestic terror plot stretching from 2019 into 2020.

Since 2021, state legislatures have pursued bills that define crimes related to unlawful entry into critical infrastructure facilities, protect additional types of energy infrastructure, and increase the penalties associated with those offenses. Many of these laws are designed to prevent disruptions of important fuel and energy resources.
In 2020, at least six states enacted policies to strengthen protections of energy infrastructure. That trend continued in 2021 and 2022, with at least 10 states either enacting or considering legislation to enhance protections for physical infrastructure, or increasing associated penalties for trespassing, vandalism, or other offenses against energy infrastructure. The total number of states that have enacted such legislation for critical and energy infrastructure protection now stands at 18.

**Protecting Energy Infrastructure**

States with laws creating or enhancing penalties related to trespassing or damaging energy infrastructure (enacted since 2018).

----

**BILLS FOCUSED ON PHYSICAL INFRASTRUCTURE PROTECTION**

- **Alabama SB 17** (enacted, 2022) creates new penalties for trespassing on critical infrastructure sites, including pipeline infrastructure and electrical power generation facilities, via unmanned aircraft systems (drones). Previous legislation on this issue (HB 516) failed in 2021.

- **Arkansas HB 1321** (enacted, 2021) includes additional types of energy and utility infrastructure in the definition of “critical infrastructure,” and creates harsher penalties for trespassing or causing damage to critical infrastructure.

- **Illinois HB 2926** (pending, 2021) would require the Illinois Commerce Commission to provide a strategic plan for hardening critical infrastructure from threats including sabotage and subversion.

- **Kansas SB 172** (enacted, 2021) creates the crimes of trespassing on a critical infrastructure facility and criminal damage to a critical infrastructure facility. Previous state law was narrowly tailored toward pipelines, rather than the broader “critical infrastructure.”

----
Montana HB 481 (enacted, 2021) establishes civil and criminal penalties for trespassing on or damaging critical infrastructure facilities, exempting activities allowed under federal law.

New Jersey AB 717 (pending, 2022) focuses on nuclear facility protection, and would make it a third-degree crime to trespass at the site of a nuclear plant, which carries higher penalties than trespassing on other critical infrastructure or utility-owned properties.

Ohio SB 33 (enacted, 2021) expands protections for critical infrastructure and increases penalties by designating tampering with critical infrastructure facilities as a third degree felony, creating higher penalties for trespassing on critical infrastructure facilities and imposing civil liabilities and fines for offenses. Ohio SB 288 (pending, 2022) would further strengthen protections and penalties if enacted.

PROTECTING ENERGY AND UTILITY WORKERS

In addition to protecting energy infrastructure from human threats, there were also new actions to protect facilities and workers, particularly from health hazards. The pace of these proposals dropped significantly after initial action at the onset of the pandemic. A few states have taken new action and at least one introduced legislation in 2021 to specifically protect utility workers from future health hazards as COVID-related impacts continued in 2021 and into 2022.

Highlighted by difficulties in securing testing, personal protective equipment, and vaccine prioritization for essential energy workers, COVID-19 severely disrupted the energy sector between 2020 and 2022. States’ efforts to protect utility workers shifted accordingly to focus on the public health threat early in the pandemic, with activity slowing down after an initial surge. Many of these pandemic-related actions are covered in detail in NCSL’s Energy Policy Response to COVID report.

Maryland HB 581 (enacted, 2021) mandates that employers develop safety protocols, provide equipment for essential workers and allow them to take additional leave if sick or symptomatic.

New York SB 640 (pending 2021) and SB 519 (pending 2021), together would establish an “essential workers bill of rights” and provide essential workers, including utility workers, with hazard pay during states of emergency.

At least one state passed legislation to further protect workers from physical hazards and threats, following a reported rise in violence against utility workers in past years. Other states have taken similar action in past legislative sessions, though we have seen less action on this specific issue between 2021 and 2022.

Idaho SB 1321 (enacted, 2022) provides further protection of utility workers by making assault on a utility worker a felony on par with assaulting a peace officer, firefighter, EMS personnel, or other similar public service official, and laying out specific penalties.
Conclusion

The security of energy infrastructure has continued to be a priority for state legislatures, especially in the wake of major cyberattacks that continue to evolve at rapid pace causing economic disruptions. State legislatures are taking a range of approaches to deal with these evolving threats, with one constant: lawmakers are playing a leading role to protect America’s energy system and will continue to lead the way on energy security policy in the years ahead.

Subsequent installments of this report will explore legislation enacted since 2021 aimed at enhancing the reliability and resilience of energy systems and facilitating a rapid response and restoration of service in the face of natural disasters.
This resource was developed under an agreement with the U.S. Department of Energy’s Office of Cybersecurity, Energy Security, and Emergency Response under award number DE-CR00000010. NCSL gratefully acknowledges the U.S. Department of Energy’s support in developing this publication.

Disclaimer: This publication 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.