Issue Brief

NATIONAL GOVERNORS ASSOCIATION

States' Role in Addressing Foreign Threats in U.S. Critical Energy Infrastructure Sectors

Executive Summary

The safety and economic security of the United States are dependent on the integrity of the nation's critical energy infrastructure systems, including power, natural gas, and petroleum. Failure of critical assets in any of these systems could have catastrophic impacts on communities, businesses and national defense. Energy is also the backbone of all other critical infrastructure systems, meaning that an energy supply failure could have cascading effects on transportation, water, telecommunications, finance, healthcare and other sectors.

While all energy infrastructure is important, critical energy infrastructure can be defined as physical or virtual energy systems and assets so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, economic security, public health or safety, or any combination of those matters. These consist of energy generation/production, transmission, and distribution systems that power hospitals, wastewater treatment plants, communications towers, food distribution facilities, residential communities, and defense installations, and are key targets of foreign cyber adversaries. Successful cyber-attacks from our nation's foreign adversaries against energy systems could undermine the continuity of business and government operations, destabilize local economies, and even jeopardize public health.

To deter, detect, and defend these entities requires the cooperation of state government along with federal interagency partners and energy sector entities. Governors are uniquely positioned to convene these stakeholders and implement policies that address these threats. This issue brief will examine the vulnerabilities of critical energy infrastructure sectors and assets to foreign threats and identify possible Gubernatorial actions to address those vulnerabilities.

Background

Foreign physical and cyber threats to energy systems have increased in complexity and sophistication, increasingly targeting critical energy infrastructure and key resources. Foreign adversaries do not have to disrupt energy supplies directly to have an impact either. For example, according to the U.S. Government Accountability Office, the SolarWinds cyberattack, believed to be perpetrated by the Russian Foreign Intelligence Service, shows the clandestine methods of adversaries that undermined the security of operational systems.[1] Vulnerabilities that remain unaddressed in critical energy infrastructure and key resources endanger the nation's security, public health and safety, and economic vitality.

Our nation's foreign adversaries employ various tactics, techniques and procedures, and use tools such as malware, ransomware, and distributed denial of service attacks. Attackers also directly target company insiders to gain access to operational and informational technology systems. Tactics can also include physical attacks on the transmission and distribution assets, particularly those powering critical end uses such as defense installations, government facilities and hospitals. These adversaries and strategic competitors have sought to attack these systems to seek political, economic, and military advantage over the United States.

> Multiple foreign adversaries have the capabilities of launching remote cyberattacks, according to the director of the Department of National Intelligence. For example, China has the ability to launch cyber-attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States. Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries. Iran's expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of the United States and allied networks and data. Iran has the ability to conduct attacks on critical infrastructure and conduct influence and espionage activities.

This issue brief was informed by the National Governors Association Center for Best Practice's *Experts Roundtable on the States' Role in Addressing Foreign Influence Threats in U.S. Critical Energy Infrastructure Sectors*, held in conjunction with the Spring Meeting of the Governors Homeland Security Advisors Council on April 6-8, 2021.

Participants sought to examine the foreign threats to U.S. critical energy infrastructure security and identify the roles and responsibilities of state and territory leaders to combat these threats. At this meeting, state, federal and industry representatives participated in discussions to explore the following topics:

1. Understanding persistent and emerging threats to U.S. critical energy infrastructure;
2. Strengthening state, private sector and federal partnerships to detect, deter and counter foreign threats; and
3. Protecting and responding to threats to the energy supply chain in the U.S.

Roundtable participants identified the following actions that states can implement to address foreign threats to critical energy infrastructure:

- Strengthen information sharing frameworks with industry and federal partners. Information such as potential or realized threats, system vulnerabilities, and mitigation and protection measures that can be implemented.
- Improve bi-directional communication with energy companies and federal partners to build trust in advance of an incident.
- Identify and prioritize assets and essential systems for energy security, including those that may be targets for foreign adversaries, and coordinate those prioritizations with the energy sector.
- Host regular energy security exercises with industry and federal partners to solidify roles and responsibilities, identify information sharing needs, and optimize response and recovery coordination.
- Perform supply chain risk management on state-procured, state-funded, and state owned or operated grid-connected assets to safeguard those technologies and services.

Policy Recommendations for Governors

Protecting the nation's critical energy infrastructure requires robust partnerships between federal interagency partners and state, local, territory and tribal authorities and the energy sector. Private and public sectors partnerships require a commitment of time, resources and trust to ensure effective and efficient information sharing among critical energy infrastructure owners and operators. This section outlines strategies that Governors can employ to address and improve critical energy infrastructure protections from foreign threats.

1. **Strengthen information sharing frameworks with industry and federal partners**

   Critical energy infrastructure information sharing better prepares all stakeholders to assess and address vulnerabilities, understand potential incident consequences, and prevent, protect against, mitigate, respond to and recover from threats and attacks. Governors, working with energy offices, homeland security, utilities, and other key entities may consider strengthening and expanding existing critical information exchanges to share threat, incident, vulnerability, and risk data with partners, including providing owners and operators with actionable information and security best practices.

   Several venues for information exchange that can be leveraged include:

   State Fusion Centers

   State fusion centers serve as focal points for the receipt, analysis, gathering and sharing of threat-related information. The fusion centers allow for two-way intelligence and information flow between the federal government and state, local, tribal and territorial, and private sector partners. Governors can work with intelligence personnel to provide information and analysis that directly responds to the needs of state officials and the energy sector, with fusion centers as the venue for such information exchange. Governors can also make sure that qualified state energy officials are able to access this information and share unclassified information with others who have a need to know.

   Information Sharing and Analysis Centers

   Information Sharing and Analysis Centers (ISACs) serve as coordinating bodies that facilitate information flow across private sector entities and with the government. The threat information synthesized and disseminated by ISACs helps infrastructure owners and operators – along with government partners – effectively protect against physical and cyber security threats.

Energy sector threat information is disseminated through three distinct, sub-sector specific information centers: The Electricity Information and Sharing and Analysis Center, the Downstream Natural Gas Information Sharing and Analysis Center, and the Oil and Natural Gas Information Sharing and Analysis Center. State officials with a need to know may be able to sign up for alerts through these information centers to maintain situational awareness. Governors can identify who has access to the state information center, as well as who has access to the multi-state information sharing and analysis centers, as those individuals can be conduits for information dissemination within the state.

U.S. Department of Homeland Security's Protective Security Advisor Program

Protective security advisors are trained critical infrastructure protection and vulnerability mitigation subject matter experts who are available to advise state and local officials as well as critical infrastructure owners and operators. These entities conduct security and resilience surveys and assessments through a range of methods and tools, including assist visits, Infrastructure Survey Tool, Rapid Survey Tool, and the Regional Resiliency Assessment Program.

Informal Information Sharing

In addition to the formal information sharing mechanisms, Governors can establish informal mechanisms and forums through which utility partners can share unclassified threat intelligence, incidents and mitigation strategies with stakeholders. These can be through undocketed, off-the-record conversations between officials or more structured reporting requirements established by legislation or the state's utility commission. If these methods are to be pursued, it is important that critical energy infrastructure information, personally identifiable information, and other sensitive information be shielded from public disclosure laws. According to an earlier NGA analysis, more than half of states currently have such protections in place for critical energy infrastructure information.[2]

2. Improve bi-directional communication with energy companies and federal partners to build trust in advance of an incident.

A whole of government approach is needed across federal, state, local and tribal authorities along with industry partners to identify and mitigate foreign threats. Governors may consider strengthening these partnerships by improving information sharing to understand threats better, enabling timely warning, and promoting increased threat awareness across their state or territory. By sharing threats, incidents and vulnerabilities, critical energy infrastructure owners and operators can more effectively and efficiently determine mitigation strategies.

Provided below are examples of actions states and territories may consider to strengthen partnerships and improve information sharing:

- Designate controlled unclassified information as critical electric infrastructure information to support and encourage information sharing between government and electric utilities.
- Establish formal partnerships with utilities to facilitate coordination, standards, awareness and communication between critical infrastructure owners and operators.
- Develop and implement standards for information sharing to safeguard and manage risk. Common standards provide critical energy infrastructure owners and operators with repeatable, interoperable and trusted information templates.

3. **Identify and prioritize assets and essential systems for security improvements, in coordination with the energy sector.**

Reliable energy supply for public health and safety facilities, military assets, and other critical infrastructure systems is paramount. Protection of these assets should be guided by a collaborative state and industry prioritization that accounts for those assets most needed for health, safety and economic performance. To do this, Governors, in coordination with other state and local entities, can identify critical state and local assets that, if offline, would have the most severe consequences and should be prioritized for resilience and security measures or expedited emergency support and restoration. These prioritizations can then be communicated to energy companies for alignment with those companies' response and restoration plans where possible. It should be noted that there is a necessary technical order to power restoration that may restore some assets before others for reasons other than risks posed, so flexibility will be needed when working with utilities on these prioritizations. The Edison Electric Institute suggests for assets that cannot be elevated in the restoration queue, Governors can consider funding other security and resilience programs, or on-site backup generation and storage so those facilities can remain online should an incident occur. Restoration can also be complicated by the physical damage caused by an event that blocks roadways and/or temporarily impedes restoration crew access to prioritized assets.

4. **Host regular energy security exercises with industry and federal partners to solidify roles and responsibilities, identify information sharing needs, and optimize response and recovery coordination.**

   Private entities and local governments largely control critical energy infrastructure, making owners and operators key players in incident protection and response. Exercises between state and territory governments and private entities allow all parties to validate plans, identify gaps and practice responses to a cyberattack with physical impacts. Governors may consider improving planning and coordination by encouraging agencies to participate in exercises with private entities for future emergency incidents affecting their critical energy infrastructure.

   Several reoccurring national energy-focused exercises include:

   - **DOE Clear Path Exercise.** An annual exercise series that examines the energy sector's ability to respond to a physical and/or cyber event, restore energy services, and coordinate with private and public sector partners. The event stresses interdependencies between the energy sector and other critical infrastructure sectors.
   - **DOE Liberty Eclipse.** A U.S. Department of Energy cybersecurity-focused exercise series. This event tests the cyber preparedness of the energy sector and Government partners by integrating emergency response coordination, information sharing, and hands-on simulations.
   - **DHS CISA Cyber Storm.** A biennial exercise to strengthen cyber preparedness in the public and private sectors. The exercise tasks participants with discovering and responding to a large, coordinated cyberattack affecting U.S. critical infrastructure.
   - **NERC GridEx.** A biennial exercise to provide the electric sector, government agencies, and other relevant organizations an opportunity to exercise emergency response plans, cross-entity coordination and information sharing, and recovery plans in response to simulated cyber and physical attacks on electric infrastructure. This distributed-play event takes place across North America and provides an opportunity for states across the country to participate alongside their electric utilities and other key partners.

Exercise Planning Resources:

- The Federal Emergency Management Agency's Homeland Security Exercise and Evaluation Program provides "a set of guiding principles for exercise and evaluation programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning."
- The Cybersecurity and Infrastructure Security Agency provides full-service exercise planning and support, including pre-event planning, exercise facilitation, scenario-development, and after-action assessments and reporting.
- The National Association of Regulatory Utility Commissioners released a state-focused Cybersecurity Tabletop Exercise Guide to help state public utility commissions design and host exercises that test utilities' cybersecurity preparedness and the efficacy of state-utility coordination and information sharing during an incident.[3]
- The National Emergency Management Association and state of **Idaho** published the situation manual for the NEMA-Idaho Petroleum Shortage Tabletop Exercise. This manually provides an instructive example for how an energy-focused, state-lead exercise can be planned, conducted, and assessed and can be tailored for other state use.[4]
- The U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response maintains an exercise library to compile and disseminate resources from past exercises. These resources can provide guidance on how best to structure future energy security exercises as the state or regional level.

5. **Perform supply chain risk management assessment on state-procured, state-funded and state owned or operated grid-connected assets to safeguard those technologies and services.**

States and territories may rely on third-party vendors like energy service companies and technology vendors, contractors, service providers, or suppliers for state-procured or funded energy technologies, such as for on-site energy generation and storage technologies, electric vehicle chargers, facility energy management systems and smart appliances. States and territories may also provide grant funding and financing to local governments, private entities and households to offset the up-

front purchase costs for these energy technologies. Possessing a large third-party ecosystem can increase the risk exposure of states and territories to foreign threats if their facilities and systems are not secure. Governors may consider adopting and expanding their third-party risk management program to administer their third-party relationships more efficiently and understand these entities' risk profiles and performance. Provided below are examples of actions states and territories may consider to manage risks posed by third-party vendors:

- Change procurement rules and contract agreements to protect the strategic objectives of the state or territory and protect against liability;
- Require compliance with the latest cybersecurity and supply chain standards and employ a third-party entity to verify compliance;
- Negotiate data security and breach requirements to outline notification requirements and specific steps to remedy an incident;
- Perform regular risk assessments and continuous monitoring to ensure entities are applying the proper controls and take actions to address vulnerabilities;
- Require a software bill of materials that lists the components in your systems to ensure components are up to date and identify vulnerabilities quickly.[5]

Conclusion

Protecting critical energy infrastructure and assets is paramount to the functioning of the United States economy and communities. Governors serve an important role in deterring, detecting and defending against foreign actors who may seek to exploit vulnerabilities in the energy sector for their gain. The strategies outlined in the issue brief are not an endpoint but a starting place for how Governors can support continuity of business and government operations dependent on the energy sector. By following these strategies, Governors can maximize the sustainability of their critical energy infrastructure sectors, including transportation, communications, finance, and health care. Importantly, protecting critical energy infrastructure and assets makes for a more resilient country and ensures the long-term fidelity of the United States homeland security mission.

Authors
Carl Amritt
Senior Policy Analyst (former)
NGA Center for Best Practices

Dan Lauf
Program Director, Energy
NGA Center for Best Practices

Michelle Woods
Program Director, Homeland Security (former)
NGA Center for Best Practices

Acknowledgments
The National Governors Association Center for Best Practices would like to thank the participants in the Experts Roundtable on the States' Role in Addressing Foreign Influence Threats in U.S. Critical Energy Infrastructure Sectors, including Brandi Martin, U.S. Department of Energy; Kristin Nordin, U.S. Department of Energy; Jason Pazirandeh, U.S. Department of Energy; Ben Deering, Office of the Director of National Intelligence; Eric Rollison, U.S. Cybersecurity and Infrastructure Security Agency; Jonathan Nuñez, Commander, State of California; John Bryk, American Gas Association; Scott Aaronson, Edison Electric Institute; Joyce Corell, Office of the Director of National Intelligence; Jonathan Bransky, Dominion Energy; and Michael Holko, Pennsylvania Public Utility Commission who contributed their expertise towards the development of this issue brief and the U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response for their generous support of this project.

Suggested Citation
Amritt C, Lauf D, Woods M. (2022 February). An Issue Brief on the States' Role in Addressing Foreign Threats in U.S. Critical Energy Infrastructure Sectors. Washington, DC: National Governors Association Center for Best Practices.

Disclaimer

This material is based upon work supported by the U.S. Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response under Award Number DE-OE0000817.

[1] U.S. Government Accountability Office. *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic).* April 22, 2021. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

[2] A critical electric infrastructure information designation exempts the information about physical and virtual assets of the bulk-power system from public release under the Freedom of Information Act and other laws requiring government disclosure of certain information or records. https://www.energy.gov/oe/critical-electric-infrastructure-information

[3] Costantini, Lynn and Raffety, Ashton. *Cybersecurity Tabletop Exercise Guide Version 1.1.* October 2021. National Association of Regulatory Utility Commissioners. https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

[4] National Emergency Management Association. *Situation Manual (SitMan) for the Idaho Petroleum Shortage Tabletop Exercise (TTX).* July 15, 2021. NEMA-Idaho Petroleum Shortage TTX SitMan (4).pdf

[5] https://www.ntia.gov/SBOM