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 other critical infrastructure systems, meaning that an energy supply failure could have cascading effects on transportation, water, telecommunications, finance, healthcare, and more. 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, among others.

Additionally, there is a subset of critical energy infrastructure referred to as defense critical electric infrastructure (DCEI). DCEI is comprised of electric infrastructure that serves critical defense facilities but is not owned or operated by those facilities. These facilities are vital to both national security and homeland defense.

Critical energy infrastructure systems are key targets of foreign cyber adversaries. Successful cyberattacks 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. In recent years, there has been increased activity by foreign adversaries using gray zone tactics, prepositioning themselves within critical infrastructure, and perpetrating opportunistic attacks, such as attacks during natural disasters. While these threats are ever-present, there is the potential for increased activity during times of heightened conflict.

To deter, detect, and defend against these entities requires coordination between state and federal 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.

** Gray zone tactics refer to activities that fall on the spectrum between peaceful relations and armed conflict. These can include influence operations, cyberattacks, and other coercive or subversive actions.*

Background: The Nature of the Threat

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 Cybersecurity and Infrastructure Security Agency (CISA), a People's Republic of China state-sponsored cyber threat often referred to as Volt Typhoon* prepositioned itself to enable disruptive or destructive cyberattacks against U.S. critical infrastructure in the future. The threat actor has primarily used living off the land techniques – a set of tactics where threat actors embed themselves in systems and operate discreetly to evade detection – o infiltrate the communications, energy, transportation, and water and wastewater sectors. Volt Typhoon has already compromised the information technology environments of multiple critical infrastructure organizations in U.S. states and territories.

Our nation's foreign adversaries employ various tactics, techniques and procedures, and use tools such as malware, ransomware, and distributed denial of service attacks, among others. Attackers also directly target company insiders to gain access to operational and information technology systems. Tactics can also include physical attacks on pipelines or electric transmission and distribution assets, particularly those serving critical end uses such as defense installations, government facilities and hospitals. Additionally, as adversaries continue to build out their artificial intelligence (AI) capabilities, there is potential for those tools to be used to increase the number, frequency, and effectiveness of cyberattacks.

Adversaries also target the public by spreading disinformation via social media and deceptive news sites to further capitalize on energy emergencies. The spread of incorrect or false information can lead to confusion which can further exacerbate an emergency as people are unsure what instructions to follow or where to get information. This discord can rapidly erode public trust and impede restoration activities.

Adversaries and strategic competitors have sought to attack these critical energy infrastructure systems in an attempt to gain political, economic, and military advantage over the United States. Governors and their states and territories are finding themselves on the front lines of these attacks, and they are using the policy and regulatory tools at their disposal to fight back and make critical energy infrastructure more hardened and resilient.

This issue brief was originally 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, April 6-8, 2021. It was updated in 2026 to incorporate new trends in tactics, techniques, and procedures as well as changes to the threat environment.

Multiple foreign adversaries have the capabilities of launching sophisticated cyberattacks, according to CISA. For example, China is capable of launching cyberattacks 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 has the ability to conduct attacks on critical infrastructure and conduct influence and espionage activities, and affiliated actors have recently targeted U.S. water and wastewater systems facilities. North Korea also has the capacity to conduct targeted attacks against critical infrastructure sectors, including previously organizing ransomware campaigns against Healthcare and Public Health Sector (HPH) organizations and other critical infrastructure sector entities.

** Other names for this threat actor are BRONZE SILHOUETTE, Vanguard Panda, DEV-0391, UNC3236, Voltzite, and Insidious Taurus*

Policy Recommendations for Governors

Protecting the nation's critical energy infrastructure requires robust partnerships between federal interagency partners and state, local, territorial, and tribal authorities in addition to the energy sector. Private and public sector partnerships require a commitment of time, resources, and trust to ensure effective and efficient coordination and cooperation 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.

Strengthen information sharing frameworks with industry and federal partners

A whole of government approach is needed across federal, state, local, and tribal authorities along with industry partners to identify and mitigate foreign threats. Timely sharing of critical energy infrastructure information better prepares all stakeholders to assess and address vulnerabilities, understand potential incident consequences, and more effectively and efficiently prevent, protect against, mitigate, respond to and recover from threats and attacks.

The key to information sharing is building, maintaining, and, where possible, institutionalizing trusted relationships and critical information sharing pathways. 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. It may be useful for Governors' advisors to be aware of opportunities for government and industry officials to engage with ISACs.

Energy sector threat information is disseminated through three distinct, sub-sector specific information centers. The Electricity Information and Sharing and Analysis Center shares threat and incident information with industry partners. State officials, including from the Governor's office, energy office, emergency management, and homeland security staff, can sign up for alerts to maintain situational awareness. Additionally, industry partners in the relevant sectors can join the Downstream Natural Gas Information Sharing and Analysis Center and the Oil and Natural Energy Information Sharing and Analysis Center; however, these have historically not been open to state participation. There are additional ISACs, such as the Multi-State Information Sharing and Analysis Center, which focus on state, local, tribal and territorial governments and may also have useful information on these threats. ISACs can be an important conduit for energy officials to obtain ongoing threat information that can be used to advance their security posture as well as to maintain situational awareness across the sector.

Subsector Coordinating Councils

The Electricity Subsector Coordinating Council (ESCC) and the Oil and Natural Gas Subsector Coordinating Council (ONGSCC) are the principal liaising entities between senior sector leadership and Federal governmental entities on issues related to energy security. The ESCC includes CEOs and other senior leaders from across the energy sector, providing them with venues to coordinate with government partners and one another in advance of and during energy emergencies. The ONGSCC serves a similar function, but with membership including senior security leaders from the sector focused on oil and gas delivery.

Co-chaired by the U.S. Department of Energy and the U.S. Department of Homeland Security, the Energy Government Coordinating Council (EGCC) provides an avenue for the ESCC and ONGSCC to partner and share information directly with government partners, including state entities like Governors' offices, State Energy Offices, and regulatory utility commissions.

Federal Information Sharing Efforts

There are a number of federal programs to facilitate information sharing. CISA regularly shares cyber threat indicators via its Automated Indicator Sharing initiative as well as through programs such as the Joint Cyber Defense Collaborative and the Joint Ransomware Task Force. The agency also has protective security advisors and cyber security advisors who are trained critical infrastructure protection and vulnerability mitigation subject matter experts and are available to advise state and local officials as well as critical infrastructure owners and operators. InfraGard, a public-private partnership between the FBI and the private sector, is another federal program aimed at better protecting critical infrastructure through education, relationship building, and information sharing. The Department of Energy started a public-private partnership pilot in 2023 called the Energy Threat Analysis Center (ETAC) to strengthen the energy sector by convening experts from the public and private sectors as well as national laboratories to better secure critical infrastructure and support response to threats. Additionally, the Department of Energy and the Electricity Information Sharing and Analysis Center run the Cybersecurity Risk Information Sharing Program (CRISP) which bidirectionally shares information on cyber threat actors and emerging trends across the sector.

In addition to formal information sharing mechanisms, Governors can establish informal mechanisms and forums through which utility partners can share threat intelligence, incidents, and mitigation strategies with stakeholders. These can be through meetings, working groups or councils, or in some instances, through more structured reporting requirements established by legislation or the state's utility commission. If these methods are to be pursued, it is important that states are mindful of public disclosure laws and how they will handle critical energy infrastructure information, personally identifiable information, and other sensitive information to avoid creating additional vulnerabilities. According to an earlier NGA analysis, more than nearly two-thirds of states and territories currently have such protections in place for critical energy infrastructure information.

Actions states and territories may consider to strengthen partnerships and improve information sharing include:

- Designate certain 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.

Identify critical system interdependencies and prioritize assets

Reliable energy supply for public health and safety facilities, telecommunications, water and wastewater facilities, military assets, and other critical infrastructure systems is paramount. Many critical infrastructure systems are interdependent, and the consequences of a single energy outage can cascade to multiple other critical infrastructure systems across the sectors. On the other hand, energy facilities are also vulnerable to impacts of other interconnected critical infrastructure being compromised. A cyberattack on another critical infrastructure sector could spread to energy facilities if their systems touch those of the affected organization.

Protection of critical assets is generally 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' offices, 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 share those with relevant stakeholders to aid in prioritization for resilience and security measures. Restoration must follow specific sequences to respect the physics of the grid, so there may be limitations to any restoration prioritization that the utilities can provide. It is important to consider how this information is shared in order to avoid creating inadvertent security vulnerabilities. As discussed above, many states have their own laws or policies regarding protection of Critical Energy Infrastructure Information. Additionally, the federal government offers protection of certain information shared with the government on infrastructure security through the Protected Critical Infrastructure Information (PCII) Program. States have an identified PCII manager who can assist them in appropriately protecting this information. In addition to mapping interdependencies across critical assets within a state, it may also be helpful to assess where out-of-state resources interact with in-state critical facilities. In many cases, energy resources, such as power and liquid fuels, come into critical facilities from across state borders. Understanding where these interdependencies exist and maintaining awareness of the conditions at the point of origin of those power assets are necessary for informed decision-making around prioritization and restoration.

Another factor to consider when identifying assets is foreign land ownership near critical infrastructure. Many states have passed laws over recent years regarding foreign acquisition of land near critical infrastructure facilities. In addition to reporting and registration requirements, some states have adopted restrictions on the new purchase of

land by foreign entities and others have directed divestment of land previously purchased by such entities. Resources on asset identification and prioritization:

- **CESER: Cross-Sector Interdependency Diagrams** – This resource shows key interdependencies between the energy sector and other critical infrastructure sectors.
- **CESER: Energy Supply Chain Diagrams** – This resource contains energy supply chain diagrams for electricity, liquid fuels, propane, and natural gas.
- **Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators** – This guidance outlines a process for owners and operators of operational technology to create an asset inventory, enabling organizations to maintain accurate and updated records of their operational technology (OT) assets.
- **NIST: Asset Management for the Energy Sector** – This guidance from NIST provides information for energy organizations on managing, monitoring, and baselining OT assets.

Incorporate Defense Electric Critical Infrastructure into your state or territory's energy security planning.

Defense installations and facilities are common targets of foreign adversaries as they lead the nation's defensive and offensive operations against nation-state threats. These facilities have increased security measures to harden them against threats, but they are still interconnected to their communities and other critical infrastructure systems and can be impacted by incidents and events within those communities and systems. It is important to find ways to incorporate defense facilities into the information sharing process on potential threats to form a common threat picture.

Identifying the DCEI in a state or territory and incorporating those facilities into the energy security planning helps to create a shared understanding of interconnected facilities and can streamline response if an incident occurs. States and territories can work with defense installation commanders to identify defense critical infrastructure and the important energy infrastructure that supports those systems. In addition to identification of assets, these efforts can highlight planning assumptions for response and restoration, ways to increase threat information sharing and intelligence, and opportunities to exercise a coordinated response to incidents that include an energy emergency. Additionally, states and territories may be able to incorporate DCEI into considerations on initiatives to strengthen energy security. In some instances, there may

be federal grants or programs, such as the Defense Community Infrastructure Program, available that enable hardening of energy infrastructure vital to both military facilities and states.

States and territories may also consider standing up a working group or regular touch points to share information, increase coordination, and institutionalize relationships between agencies that can withstand personnel turnover. Where possible, including DCEI energy providers in these working groups can aid in increased hardening, resiliency, and coordination. Even if state and energy personnel engaged in these efforts have security clearances, installations may have limitations in what information they are able to share based on its level of classification and ability to impact national security. Building trusted, ongoing partnerships and joint planning efforts can help to find creative solutions (e.g., ways to identify priority, emphasis, or interest) to collectively increase security and facilitate a more coordinated response without putting key assets at increased risk.

Resources on DCEI:

- The Department of Energy's (DOE) Strengthening the Resilience of Defense Critical Electric Infrastructure is a 2021 report that offers recommendations for federal entities on DCEI; some recommendations require partnership with other industry stakeholders.
- The National Association of Regulatory Utility Commissioners (NARUC) has a set of resources on Defense Community Partnerships that offer guidance on defense energy resilience for regulators.
- The Department of Defense's Office of Local Defense Community Cooperation has resources including information on grants through the Defense Community Infrastructure Program which helps states and localities to address deficiencies in community infrastructure supportive of a local military installation.

Host regular energy security exercises that factor in foreign adversary threats with industry and federal partners to solidify roles and responsibilities, plan communications strategies, 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. Collaborative exercises that include federal entities, state and territory governments, and private entities allow all parties to validate plans, identify gaps and practice responses. 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. Exercises are also critical for DCEI as they provide an opportunity for all relevant stakeholders to coordinate the roles they play in the protection of this key infrastructure.

Additionally, it is important to exercise how to communicate during an energy crisis. Energy emergencies may affect telecommunications access for some impacted. In some instances, it may be necessary to share public safety information to reduce loss of life and property. Recent attacks on critical infrastructure have also highlighted how threat actors capitalize on these events and spread mis- and disinformation to further exacerbate the situation. Having a communications plan in place and exercising that communications plan can streamline messaging which can go a long way to implementing a quick and effective response to an emergency.

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**. An annual 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 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.

- The National Emergency Management Association and state of Idaho published the situation manual for the NEMA-Idaho Petroleum Shortage Tabletop Exercise. This manual 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.

- 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 at the state or regional level.

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 of 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. Choosing vendors and products that factor in security during the design phase can help protect against threats by minimizing the opportunities for exploitable flaws.

Provided below are examples of actions states and territories may consider to manage risks posed by third-party vendors:

- Evaluate procurement rules and contract agreements and make changes as needed 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, limit systems access to only those who need it for functionality and continuously monitor to ensure entities are applying 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

Supply Chain Resources:

- **CISA Supply Chain Resource Library** has a list of resources and information on supply chain programs, rulemaking, and other activities to support supply chain risk management efforts
- **ODNI NCSC Supply Chain and Cyber Directorate** put out a series of guides and resources aimed at enhancing supply chain security.
- **CISA Minimum Elements for a Software Bill of Materials** provides guidance on Software Bill of Materials elements and implementation to help organizations to better identify vulnerabilities, assess risk, and make informed decisions about the software they use.
- The Department of Defense resource on **Foreign Ownership, Control, or Influence** (FOCI) describes how the department is addressing these risks, types of FOCI risk, and how to mitigate.

Conclusion

Protecting critical energy infrastructure and assets is paramount to national security. Governors serve an important role in enacting policy to deter, detect, and defend against foreign actors who seek to exploit vulnerabilities in the energy sector for their gain. The strategies outlined in the issue brief are a starting place for ways Governors can support continuity of business and government operations dependent on the energy sector. By following these strategies, Governors can maximize the readiness and resilience of their critical energy infrastructure systems. Importantly, protecting critical energy infrastructure and assets makes for a more resilient country and ensures the long-term fidelity of the U.S. homeland security mission.

Disclaimer

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