



NASEO

National Association of
State Energy Officials

Enhancing Energy Sector Cybersecurity: Pathways for State and Territory Energy Offices

2020

Disclaimer

This material is based upon work supported by the U.S. Department of Energy under award number DE-OE0000810. This report was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof.

Acknowledgments

The National Association of State Energy Officials (NASEO) thanks the following individuals for their contributions to and review of this report: NASEO Energy Security Committee Co-chairs Ben Bolton, Tennessee Department of Environment and Conservation, and Megan Levy, Office of Energy Innovation, Wisconsin Public Utility Commission; the U.S. Department of Energy's Kate Marks, Brandi Martin, and Ashton Raffety; and NASEO's Shemika Spencer, Sandy Fazeli, and Kirsten Verclas.

This report was co-authored by NASEO's Campbell Delahoyde, Senior Program Manager and Jeff Pillon, Director, Energy Assurance in 2020.

Though cybersecurity has been a long-standing issue, in 2017 the NASEO Board of Directors officially resolved to include energy sector cybersecurity in its list of organizational priorities.¹ This paper supports that commitment and will help provide context for state energy officials to understand the energy sector cybersecurity landscape and identify initial steps that can be used to identify appropriate responsibilities and build capacity to fulfill them.

¹ National Association of State Energy Officials. Board of Directors Resolution on Energy Emergency and Cyber Security Planning, Preparedness, and Response. [https://www.naseo.org/Data/Sites/1/naseo-resolution-on-energy-emergency-planning-\(final-42717\).pdf](https://www.naseo.org/Data/Sites/1/naseo-resolution-on-energy-emergency-planning-(final-42717).pdf). April 27, 2017.

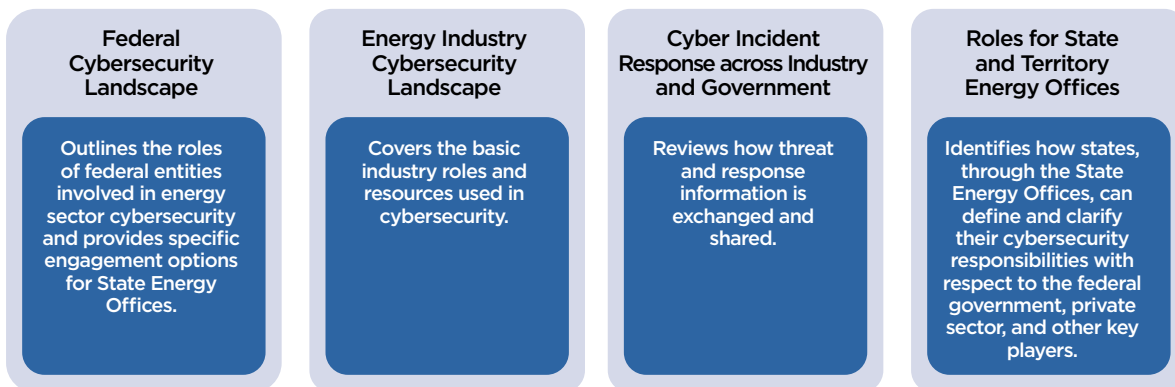
Contents

Executive Summary	4
Federal Cybersecurity Landscape for the Energy Sector	5
U.S. Department of Energy	5
U.S. Department of Homeland Security	7
Federal Bureau of Investigation	8
U.S. Department of Transportation	9
Energy Government Coordinating Council	9
Energy Industry Cybersecurity Landscape	10
Electricity Subsector Coordinating Council	10
Oil and Natural Gas Subsector Coordinating Council	10
Information Sharing and Analysis Centers	10
Cyber Incident Response: Actionable Information and Intelligence Sharing	12
Federal Doctrine	12
Summary of Information Sharing Channels between Public and Private Sectors	13
Actionable Information	15
Considerations for Sensitive Information Sharing	15
Open Government Law Exemptions for Critical Energy Infrastructure	16
Cybersecurity Roles for State and Territory Energy Offices	17
Seven Frequently Asked Questions to Help Energy Officials Determine Cybersecurity Roles:	18
Developing an Energy Sector Cybersecurity Planning and Response Strategy	20
Actions States and Territories Can Take to Improve Energy System Cybersecurity Risk Mitigation and Preparedness	21
Risk Mitigation and Resiliency	21
Coordination	22
Energy Emergency Response Planning	23
Afterword	24
Annex A: Federal Policy and Guidance	25

Executive Summary

Cyberattacks are serious threats to our nation. From ransomware targeting small businesses to advanced cyber campaigns perpetrated by foreign adversaries who seek to undermine critical infrastructure, the cyber threat landscape is vast, persistent, and evolving. As one of the most vital critical infrastructure sectors, the energy sector is at risk to all types of threats. Information technology (IT) threats can include attempts to exploit private utility customer information or hamper state government network functionality. Operational technology (OT) threats can include cyber intrusions and overrides of machinery that physically damage energy infrastructure and disrupt the flow of energy. To prevent and/or mitigate the effects of cyber-attacks and exploitations, it is important for all energy stakeholders—from individual energy providers to state and federal government agencies—to be aware of cyber threats, implement effective cyber policies and defense protocols, and develop cyber incident response plans.

Understanding and confronting cyber threats to energy infrastructure requires State and Territory Energy Officials to develop their knowledge of cyber risks and protections, strengthen their own cybersecurity policies, actions, and protocols, and build relationships with all energy stakeholders.² In response to this need, this guidance has four sections: the first three provide background on ongoing cybersecurity efforts in both the public and private sectors and identify state-relevant communication channels and mechanisms for sharing information; the fourth identifies roles State and Territory Energy Offices might play in enhancing cybersecurity and response actions. Specifically, they cover the following topics:



State Energy Offices' roles in cybersecurity vary across the nation. Some have an active or a formal role while others do not. State Energy Offices engaged in cybersecurity generally conduct the following key activities, each of which can be further broken down into policy, programs, and operations:

1. Supporting cyber risk mitigation and resiliency;
2. Coordinating within state government and across the public-private nexus; and
3. Responding to a cyberattack affecting energy infrastructure through consequence management as part of all-hazards energy assurance.

Just as cybersecurity threats are continually evolving, so, too, must states adopt approaches that are nimble and adaptive to the changing landscape. There is no “one-size-fits-all” solution, but the experience of State Energy Offices in enhancing the physical security and cybersecurity of energy infrastructure may offer important insights and best practices.

² State and Territory Energy Offices and the District of Columbia's Department of Energy and Environment, hereby referred to as “State Energy Offices”, advance practical energy policies, inform regulatory processes, and support energy technology research, demonstration, and deployment. In partnership with the private sector, State Energy Offices accelerate energy-related economic development and support meeting state climate goals through energy solutions that address their citizens' needs and enhance physical and cyber energy security.

Federal Cybersecurity Landscape for the Energy Sector

The Federal Government’s actions and commitments in energy sector cybersecurity reflect the importance and evolving nature of the threat. Through a series of presidential orders, legislation, and plans, the U.S Department of Energy (DOE) and its agency partners are directed to coordinate and strengthen preparedness and response efforts with states and industry.

State Energy Officials can engage several federal agencies to access cybersecurity resources and understand how to work together in the event of an incident. The resources identified below may be pertinent to states’ engagement of federal partners and/or to their role coordinating with industry.

U.S. Department of Energy

DOE is the sector-specific agency for partnering with states and industry on cybersecurity in the energy sector, and the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) implements this role. CESER also supports restoration and recovery for states and industry after energy disruptions resulting from natural and manmade hazards, including cyberattacks. CESER works with state, local, tribal, and territorial (SLTT) governments on energy security preparedness and through its federal Emergency Support Function 12—Energy (ESF-12) response team. CESER also performs research and development, assisting energy sector asset owners by developing cybersecurity technologies and tools to prevent, detect, mitigate, and survive cyber incidents.

CESER works closely with SLTT governments to:

- Increase awareness of hazards to the energy system and help mitigate the impacts of disruptions and make more informed response decisions.
- Improve coordination and cybersecurity emergency response among federal agencies, states, and industry.
- Enhance energy incident preparedness and response through more organized, consistent, and customizable training.

Ways to Engage DOE

- Identify the primary and secondary points of contact from the State Energy Office, Public Utility Commission (PUC), and/or other relevant agencies, particularly those designated as the state [Energy Emergency Assurance Coordinator\(s\) \(EEAC\)](#). It is up to each state to designate who will serve as the EEAC. DOE and NASEO can provide information on state contacts. Leading up to and during energy disruptions, CESER shares situational awareness and coordinates among EEACs in the affected states and regions.
- Register for [EAGLE-I](#), the interactive geographic information system used to view and map energy infrastructure and obtain near real-time visual updates concerning the electric, petroleum, and natural gas sectors.
- Learn about upcoming DOE, other federal agency, and industry exercises on the Energy Sector Exercises Quarterly Forum webinar. Email exercises@hq.doe.gov to join the Forum listserv.
- Drive the next generation of energy cybersecurity professionals by encouraging university students in your state to participate in CESER’s annual, hands-on CyberForce Competition™.

In 2018, DOE released a [multiyear plan](#)³ to improve cybersecurity and resilience of the nation’s energy system. The goals relevant to states are:

<p>Strengthen Cyber Preparedness Among State and Local Stakeholders: DOE will work with state and local energy stakeholders to ensure that state energy assurance plans and associated capabilities address state and local energy needs and are consistent with regional and federal cyber efforts. Individual states have developed state-level plans for energy distribution during emergencies; these plans are living documents that should be updated regularly to address the evolving physical and cyber risk landscape. State energy assurance plans are intended to address all hazards to the energy sector; however, the majority of existing energy assurance plans do not account for cyber incidents. Cyber incidents may introduce distinct requirements or priorities that should be considered for energy assurance. To that end, DOE plans to:</p>		
<p>Increase number of states including cyber elements in their Energy Assurance Plans (EAP) from 25% to 100% by the end of FY’21.</p>	<p>Coordinate cyber incident exercises, responses and recovery efforts, processes, and protocols with industry, federal, state, and local stakeholders.</p>	<p>Provide federal and state incentives to accelerate investment in and adoption of cyber-resilient energy delivery systems.</p>

CESER Programs and Functions Supporting Cybersecurity

While the following programs were designed for utilities, State Energy Officials should be familiar with them in order to develop a shared language and understanding of energy sector cybersecurity with industry and federal partners. As state-specific subject matter experts, State Energy Officials are well-suited to share unique contextual information with industry and federal partners.

<p>Cybersecurity for Operation Technology Environment (CyOTE™)</p> <ul style="list-style-type: none"> Project demonstrating and addressing the challenges of collecting and sharing data on OT networks. Pilot results will be used to develop a repeatable, standard approach for energy industry to address operational threat data sharing and analysis. 	<p>Cybersecurity Capability Maturity Model (C2M2)</p> <ul style="list-style-type: none"> Tool designed to enable electricity, petroleum, and natural gas organizations to measure and compare their level of cybersecurity against industry averages per subsector. As part of DOE’s multiyear plan for cybersecurity, will work with national labs and industry to update and expand implementation and scope of tool to address the changing technology and risk landscape. C2M2 is based on the NIST Framework. 	<p>Cybersecurity Risk Information Sharing Program (CRISP)</p> <ul style="list-style-type: none"> Industry-sponsored partnership which facilitates timely sharing of cyber threat information and develops situational awareness tools to help the energy sector identify, prioritize, and coordinate the protection of its critical infrastructure. Provides near-real-time capability for critical infrastructure owners and operators to voluntarily share and analyze cyber threat data and receive machine-to-machine feedback on mitigative measures.
---	---	---

³ U.S. Department of Energy. Multiyear Plan for Energy Sector Cybersecurity. March 2018. https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

U.S. Department of Homeland Security

The U.S. Department of Homeland Security (DHS) is responsible for protecting the nation from all hazards. The [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) directs national efforts to protect and enhance the security and resiliency of the nation's cybersecurity, emergency communications, and critical infrastructure from physical and cyber threats in collaboration with the public and private sectors. CISA maintains a cadre of Protective Security Advisors (PSAs) who facilitate local field activities in coordination with other DHS offices to advise and assist state and local officials with critical infrastructure protection programs. Similarly, DHS has regional Cyber Security Advisors (CSAs) who support cyber components of critical infrastructure.

Ways to Engage DHS

- Get to know your regional PSA by emailing CIOCC.Physical@cisa.dhs.gov.
- Register for access to [DHS' Infrastructure Protection \(IP\) Gateway](#), which provides various data collection, analysis, and response tools to SLTT governments on a verified, need-to-know basis for qualifying and vetted applicants. Contact the IP Gateway Help Desk via email at IPGateway@hq.dhs.gov to get started.
- Contact a CSA within CISA's Infrastructure Security Division by emailing cyberadvisor@hq.dhs.gov.
- Review Best Practice Case Studies and explore the SLTT Toolkit on the [CISA Website](#).
- Contact your DHS [Regional Office](#) to learn about regional training, risk mitigation, and coordination opportunities.

In March 2018, DHS's Transportation Safety Administration (TSA) updated the [Pipeline Security Guidelines](#) to include a section titled "Pipeline Cyber Asset Security Measures"⁴ that contains planning and implementation guidance. In December 2018, TSA published the [Cybersecurity Roadmap 2018](#)⁵, which clarifies the agency's direct physical and cybersecurity oversight authority for all seven transportation systems sectors (pipeline systems, aviation, highway and motor carrier, maritime, mass transit and passenger rail, freight rail, and postal and shipping). The Roadmap also discusses its collaboration role with CISA through the [Pipeline Cybersecurity Initiative](#) which was unveiled in October 2018. The Initiative will enable pipeline owners and operators to use voluntary assessment tools to identify and mitigate potential vulnerabilities.

National Institute of Standards and Technology

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, issued in February 2013, directed the National Institute of Standards and Technology (NIST) to develop a voluntary framework for reducing cybersecurity risks in collaboration with stakeholders. [The Framework for Improving Critical Infrastructure Cybersecurity](#)⁶ provides guidance, based on existing standards, guidelines, and practices, for organizations to better manage and reduce cybersecurity risk. State Energy Officials can work with public and private energy sector stakeholders to support and encourage the use of this framework in the development of programs and initiatives, particularly when working with municipally-owned or rural cooperative utilities.

⁴ Transportation Safety Administration. Pipeline Cyber Asset Security Measures, March 2018. https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

⁵ Transportation Safety Administration. TSA Cybersecurity Roadmap 2018. December 4, 2018. https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap.pdf.

⁶ National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. April 16, 2018. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

DHS Programs and Functions Supporting Cybersecurity

National Cybersecurity and Communications Integration Center (NCCIC)	Critical Infrastructure Cyber Community C3 Voluntary Program	National Risk Management Center (NRMC)
<ul style="list-style-type: none">• Serves as a national hub for cyber and communications information, technical expertise, and operational integration. Operates a 24/7 center which provides situational awareness, analysis, and incident response and cyber defense capabilities to federal, state, local, tribal, and territorial governments. Also defends federal computer networks and responds to significant events.• State energy agencies might work through their state fusion centers to receive information on relevant threats to the state's critical energy infrastructure.	<ul style="list-style-type: none">• Supports owners and operators of critical infrastructure, academia, federal, state, local, tribal, and territorial governments, and businesses in their use of the NIST Cybersecurity Framework.• States energy agencies and offices can encourage energy suppliers to participate in this program as a way to improve their cybersecurity.	<ul style="list-style-type: none">• Planning, analysis, and collaboration center working to identify and address the most significant risks to U.S. critical infrastructure.• In supporting both emergency response and risk mitigation activities, state energy officials might use information from the NRMC to support their coordination with their state homelands security agencies.

Federal Bureau of Investigation

Under the [National Cyber Incident Response Plan](#)⁷, the U.S. Department of Justice, working through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force, is the lead agency for threat response during any significant cyber incident affecting civilian networks. The FBI sponsors InfraGard, a public-private partnership which provides information exchange and education on threats to critical infrastructure from physical and cyber threats. [InfraGard](#) is structured through local chapter memberships comprised of business officials, military and government officials, computer professionals, academia, and state and local law enforcement who contribute specific industry insight. State energy officials with cybersecurity responsibilities should consider joining local InfraGard chapters to foster relationships that could be beneficial during a significant cyber incident.

Ways to Engage the FBI

- Join your local [InfraGard](#) chapter to become part of a vetted public-private information-sharing network dedicated to protecting critical infrastructure.
- Contact [your state Bureau of Investigation's](#) Cybersecurity group to become familiar with staff, services, and key points of contact. Some state's functions are more robust than others, but range from providing basic education to responding to active cyber intrusions with teams of specialists.

⁷ U.S. Department of Homeland Security. National Cyber Incident Response Plan. December 2016. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

U.S. Department of Transportation

The U.S. Department of Transportation's (DOT) [Pipeline and Hazardous Materials Safety Administration \(PHMSA\)](#) is responsible for regulating the safety of hazardous materials transportation and the safety of pipeline systems. It has oversight responsibilities and the power to mandate protective measures, safety standards, and incident reporting. PHMSA produces official public notices which recommend protective measures in response to specific incidents, which can include cyber incidents.

As noted earlier, TSA's Pipeline Security Division oversees pipeline **security**, complementary to and distinct from the role of PHMSA, which oversees pipeline **safety**. PHMSA focuses primarily on accidents (e.g. equipment failures) affecting pipelines, whereas TSA focuses on natural and manmade hazards, including cyberattacks. The two entities operate and coordinate closely to enhance pipeline security.

Ways to Engage DOT PHMSA

- Determine if your office has any responsibility overseeing or inspecting pipeline safety and underground natural gas storage programs. In several states, this responsibility may fall to the PUC, but State Energy Offices might find it useful to understand current cybersecurity efforts in the pipeline sector

Energy Government Coordinating Council

The [Energy Government Coordinating Council \(EGCC\)](#) is composed of federal government agencies, namely DOE, DHS, CISA, FBI, PHMSA, and TSA, and state associations, including NASEO. The EGCC enables interagency and cross-jurisdictional coordination among all public members and hosts joint meetings with energy industry coordinating councils to share information, coordinate efforts, and work toward joint public-private energy sector action on risk reduction. The EGCC is co-chaired by DOE CESER and DHS CISA. NASEO represents the interests of state energy officials through the Energy Government Coordinating Council—led by DOE and DHS—and with the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council, all described further below. Through coordination with these industry-led councils, NASEO engages in bidirectional communication, conveying information about state programs and priorities to industry and federal partners and in turn informing states of federal strategies for future coordination.

Federal Energy Regulatory Commission

The [Energy Policy Act of 2005](#)⁸ gave the [Federal Energy Regulatory Commission](#) (FERC) authority to oversee the reliability of the bulk power system. This includes authority to approve mandatory cybersecurity reliability standards for the bulk electric system. The reliability policies of FERC are carried out by the North American Electric Reliability Corporation (NERC), which develops and enforces cybersecurity standards. This includes reporting standards and supply chain requirements.

⁸ Library of Congress. Energy Policy Act of 2005. August 8, 2005. <https://www.congress.gov/109/plaws/publ58/PLAW-109publ58.pdf>.

Energy Industry Cybersecurity Landscape

According to the National Infrastructure Protection Plan (NIPP), voluntary collaboration between critical infrastructure owners and operators and their government counterparts is the ideal strategy to organize and address cyber vulnerabilities, threats, and hazards. The 16 critical infrastructures delineated in the NIPP are each assigned a federal department or agency as the lead coordinator or sector-specific agency (SSA). As previously noted, DOE is the designated SSA for the energy sector.

Each designated critical infrastructure sector has its own [Sector Coordinating Council](#), which is composed of private entities and serves as the principle collaboration point between the government and the private sector for critical infrastructure security and resilience policy coordination and planning. Each sector has an Information Sharing and Analysis Center (ISAC), which disseminates information. Under the NIPP framework, the energy sector is divided into two major subsectors—Electricity, and Oil and Natural Gas—each has its own coordinating council and ISAC. Each subsector determines its own actions, priorities, and approach to public-private cybersecurity.

Electricity Subsector Coordinating Council



The [Electricity Subsector Coordinating Council \(ESCC\)](#) serves as the structural liaison between electric power industry entities and the government. Its mission is to coordinate efforts to prepare for, and respond to, national-level disasters and threats to critical infrastructure. The ESCC includes electric company executives and trade association leaders representing all segments of the electric subsector.

The ESCC is led by three co-chairs representing investor-owned, municipal, and electric cooperative utilities. This structure allows for representation from both regulated and nonregulated entities to determine high-level strategy, irrespective of regulatory and policy affairs. The ESCC also works with the government through the EGCC for the energy sector and with other energy sector partners to coordinate public-private priorities, strategies, and partnerships.

Oil and Natural Gas Subsector Coordinating Council

The [Oil and Natural Gas Subsector Coordinating Council \(ONG SCC\)](#) includes owners and operators from a number of oil and natural gas trade associations, representing all operational segments of various supply chains—drilling, exploration and production, marketing, processing, refining, service and supply, transmission, distribution, and transportation (pipeline, marine, motor, and rail). ONG SCC members work in coordination with their members and government partners to develop models, standards, and reports that address cybersecurity for the entire subsector, and for specific segments of the ONG value chain.⁹ For example, the ONG SCC encourages all ONG companies to adopt the NIST Cybersecurity Framework, which standardizes language and management procedures for all organizations regardless of size, cyber posture, or sector.



Information Sharing and Analysis Centers

The Information Sharing and Analysis Centers (ISACs) gather and analyze security data, share appropriate data with stakeholders, coordinate incident management, and communicate mitigation strategies with various respective stakeholders.

⁹ Oil and Natural Gas Sector Coordinating Council. ONG Cybersecurity 101. 2018. <http://ongsubsector.com/documents/ONG-Cybersecurity-101-Factsheet.pdf>.

Ways to Engage the ISACs

- Register for and participate in the NERC/E-ISAC bi-annual [Grid Security Exercise \(GridEx\)](#)
- Become a member of the [Multi State-ISAC \(MS-ISAC\)](#)
- Work with your [state Fusion Center](#) to potentially receive information on threats to your critical energy

Electricity, Oil and Natural Gas, and Downstream Natural Gas Information Sharing and Analysis Centers



The Electricity Information-Sharing and Analysis Center (E-ISAC), in collaboration with DOE and the ES&C, serves as the primary security communications channel for the electric industry and enhances industry's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents. The E-ISAC is operated by the North American Electric Reliability Corporation (NERC) and is organizationally isolated from NERC's enforcement processes.¹⁰

The Oil and Natural Gas ISAC (ONG-ISAC) and Downstream Natural Gas ISAC (DNG-ISAC) provide a secure and trusted environment for the sharing of cybersecurity information across the natural gas and oil industry. Through these ISACs, natural gas and oil companies share cyber threat indicators and intelligence with each other and with the U.S. government.¹¹

The ISACs facilitate bi-directional information-sharing among industry and DHS, DOE, FBI, and others. The ISACs participate in regular threat briefings with DOE.

Multi-State Information Sharing and Analysis Center

The mission of the Multi-State Information Sharing and Analysis Center (MS-ISAC) is to improve the overall cybersecurity posture of SLTT governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure and promotes two-way sharing of



information between the public and private sectors in order to identify, protect, detect, respond, and recover from attacks on public and private critical infrastructure. The MS-ISAC also works closely with other organizations, such as the National Council of ISACs, the National Governors Association (NGA), the National Association of State Chief Information Officers, state fusion centers, as well as other public and private sector entities, to build trusted relationships that further enhance the country's collective cybersecurity posture.¹² State energy officials may register as members of the MS-ISAC at no cost to receive updates on IT system cybersecurity threats and threats to critical energy infrastructure.

In 2019, the Electricity-ISAC and MS-ISAC entered into an agreement to help protect critical electric infrastructure from cyber threats via improved information sharing among members. This agreement is intended to improve coordination and cooperation between the E-ISAC, a primary recipient and conveyor of electric sector cyber threat information, and state and local governments that are members of the MS-ISAC. This agreement should help MS-ISAC members, such as State Energy Officials, state chief information officers (CIOs) or chief information security officers (CISOs), and others receive more timely and detailed threat updates on energy security issues.

¹⁰ North American Electric Reliability Corporation. Electricity Information Sharing and Analysis Center. 2017. <https://www.nerc.com/pa/CI/ESISAC/pages/default.aspx>.

¹¹ Oil and Natural Gas Subsector Coordinating Council, Natural Gas Council. Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry. 2018. <https://www.api.org/-/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf>.

¹² Center for Internet Security. MS-ISAC Charter. September 24, 2018. <https://www.cisecurity.org/ms-isac/ms-isac-charter/>.

Cyber Incident Response: Actionable Information and Intelligence Sharing

Cybersecurity threats impact all energy subsectors – electricity, petroleum, and natural gas – as well as those sectors’ interactions with other critical infrastructure such as water/wastewater, transportation, and telecommunications. Following a cybersecurity incident, as in any emergency, information is requested and distributed, and responses are coordinated via a complex network of organizations. Particularly in an emergency situation, a clear understanding of how information flows and how it is obtained is critical for a timely response or incident mitigation.

This section provides a basic understanding of the authorities and relationships that guide energy sector cyber incident coordination and response.

Federal Doctrine

The [Cybersecurity Information Sharing Act of 2015](#) authorizes and encourages private companies to take defensive measures to protect against and mitigate cyber threats. In order to encourage cyber threat information-sharing with government partners, the law includes provisions to protect companies from liability, non-waivers of privilege, and protections from the federal Freedom of Information Act (FOIA) disclosures under certain circumstances and with certain entities. Because information sharing is a key component of energy emergency response, prevention, and mitigation, it serves as enabling legislation for foundational incident response planning.

[The National Cyber Incident Response Plan \(NCIRP\)](#) is the guiding doctrine for comprehensive national cyber incident response, including states, private sector stakeholders, and international partners. It outlines the following five guiding principles:

SHARED RESPONSIBILITY	The NCIRP emphasizes the shared vital interest and complementary roles and responsibilities of SLTT governments, federal entities, and private sector partners in protecting the country from malicious cyber activity and managing cyber incidents and their consequences. Organizations have different assets, information, and authorities that contribute to a successful response. An effective response means tapping into those available resources and coordinating those resources in an effective manner. The government and sector coordinating councils, ISACs, and state fusion centers serve as coordinating entities that help share critical information and assign available resources to appropriate tasks.
RISK-BASED RESPONSE	Responses will be proportional to the identified risks posed to an entity, U.S. national security, foreign relations, the broader economy, public confidence, privacy and civil liberties, or the public health and safety of the American people. A cyber incident affecting an organization’s network, for example, might pose a lesser risk than a cyber incident affecting the functionality of critical infrastructure, thus warranting a smaller response. State officials, as local subject matter experts, are aware of unique local risks and factors that can help determine the appropriate level of response.
RESPECTING AFFECTED ENTITIES	To the extent permitted under law, federal responders will safeguard details of the incident as well as privacy, civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event of a significant cyber incident where the public interest is served by issuing a public statement concerning an incident, federal responders will coordinate their approach with the affected entities to the extent possible. For state governments, this can mean ensuring that protections exist for sensitive or proprietary information that may be requested to assist a response. These can be legislative protections or memorandums of understanding established with private entities.














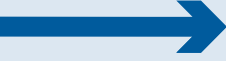
<p style="text-align: center;">UNITY OF GOVERNMENT EFFORT</p>	<p>Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be mobilized in response to cyber incidents. When responding to a cyber incident in the private sector, the concept of unity of effort synchronizes the overall federal response, which prevents gaps in service and duplicative efforts. SLTT governments also have responsibilities, authorities, capabilities, and resources that can be used to respond to a cyber incident; therefore, the federal government must be prepared to partner with and support SLTT governments in its cyber incident response efforts.</p>
<p style="text-align: center;">ENABLING RESTORATION AND RECOVERY</p>	<p>Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible. Public-private partnerships are crucial in returning to normalcy. State officials should establish reliable relationships with relevant private entities to deconflict efforts and remove hurdles that may inhibit natural and expedient recovery.</p>

The NCIRP outlines basic reporting mechanisms and resources for cyber incident management on several levels. For state consideration, the NCIRP places emphasis on state fusion centers, which are the convening mechanism for SLTT, federal, and private sector cybersecurity information sharing, coordination, and response within respective states. Generally, a state’s emergency management, homeland security, or cybersecurity agency is the primary entity responsible for representing the state. It is nevertheless important for the State Energy Office to be connected to the assigned agency, point of contact, or fusion center with respect to cybersecurity planning, as a cyber incident affecting the energy sector would require the input of energy sector subject matter experts. The NCIRP also provides an outline for developing an internal cyber incident response plan.

Summary of Information Sharing Channels between Public and Private Sectors

Information-sharing procedures are vital to understanding vulnerabilities, threats, and incident response. Energy sector cyber incident response is a constantly changing process that varies tremendously based on the state(s) in which the incident occurs, the infrastructure affected, the type of cyber threat, and the possible extent of damage. State Energy Officials are encouraged to become familiar with the foundational plans and policies guiding information sharing and cyber incident response, particularly if they have an ESF-12, consequence management, or public messaging role.

The following is a summary of some of the key means by which cyber risk information is shared. There are both one-way and two-way information flows.

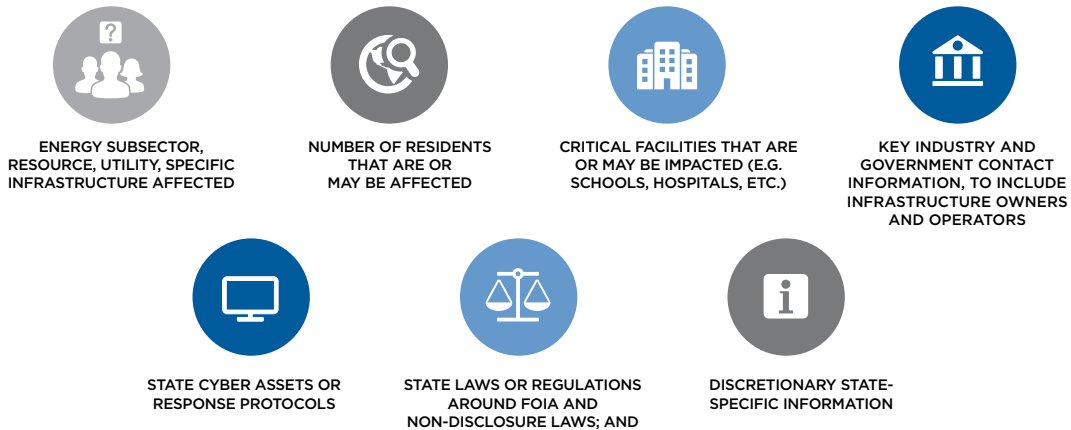
Source	Information Type	Information Flow	Recipient
DHS Homeland Security Information Network (HSIN)	Information Sharing on threats, including how analysts, investigators and private sector partners collaborate		Vetted members of federal, SLTT and Private Sector. State EEACs may request access.
FBI InfraGard Program	Threats, Attacks Vulnerabilities, Risk Mitigation		Private and public vetted membership and local chapters
State Energy Emergency Assurance Coordinators	Potential energy Supply disruptions, Incidents, events, and responses (all-hazards)		DOE/CESER/other states in the impacted region
Multi-State ISAC (Primary focus is SLTT-operated computer networks)	Threats, Attacks Vulnerabilities, Risk Mitigation		State Fusion Centers and Chief Information Officers (CIO)
Electric Utilities	OE-417 Electric Disturbance Events report		DOE, CESER
Electric Utilities	Intelligence Sharing, Threats, Attacks		E-ISAC private sector and public utilities
Electric Utilities	Threats, Attacks		NERC via critical infrastructure protection incident reporting ; DHS NCCIC
Electric Utilities	Threats, Attacks		State PUCs that have adopted rules or procedures
Oil and Natural Gas (ONG) Utilities	Information Sharing, Threats, Attacks		ONG ISAC private sector only
Natural Gas Transmission and Distribution Companies	Information Sharing, Threats, Attacks		DNG ISAC private sector only
Pipelines Operators	Incidents of abnormal operations and SCADA systems		PHMSA
DHS National Risk Management Center (NRMC)	Strategic and cross-cutting understanding of risk analysis and planning		Federal, SLTT, and private/public energy sectors including state fusion centers
DHS NCCIC, US Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems - Cyber Emergency Response Teams (ICS-CERT)	Information Sharing, Threats, Attacks and Collaboration.		Federal, SLTT, and private/public energy sectors including state fusion centers
EnergySec monthly threat briefing webinar	Threats, Attacks Vulnerabilities		State PUCs and other approved attendees

Actionable Information

In general, states should only collect critical infrastructure information that they consider actionable and necessary. In instances where a cyber breach might result in inappropriate network access or access to other company information, response actions may fall outside the purview of the State Energy Office. If a cyberattack results in a disruption of energy resources to customers, response designation may fall within the scope of an agency's duties.

The National Governors Association has developed a list of lead and supporting agencies for State Cyber [Disruption Response Plans](#) per state. NASEO recommends that State Energy Offices review their state's respective information within the report. Any information shared during a cyber incident will likely need to be protected because of its sensitive content or because there will likely be a forensic investigation into its nature and origin. Protecting information means restricting who can view it (i.e., authorized personnel, clearance holders, etc.), how it is viewed (i.e., password protected, authentication procedures, etc.), and if it is exempt from public disclosure. It is important to consider the type of information that may be needed in conjunction with respective state laws that would protect it.

The following are examples of actionable information that State Energy Officials and state ESF-12 responders may be responsible for collecting and providing to appropriate agencies and authorities during a cyber incident. This list is not exhaustive and will vary state-to-state:



Considerations for Sensitive Information Sharing

In discussions about information sharing, the question arises as to how sensitive information received can be legally protected from public disclosure. Most states have freedom of information laws or sunshine laws for which any publicly held information is subject to disclosure unless there are provisions within the law to exempt it. This is an issue of great concern to the private sector and represents a significant challenge in sharing sensitive information.¹³ If states are to receive sensitive cybersecurity information—particularly related to threats and vulnerabilities—they must have the legal and administrative processes in place to protect the information from public disclosure. For example, in March of 2018, Michigan enacted a law which categorizes sensitive cybersecurity information shared with state agencies as FOIA-exempt.¹⁴ This law and similar provisions foster greater public-private trust and enhance information-sharing and coordination during cyber incidents.

¹³ "Sensitive" in this case could include any data that is considered proprietary, contain personally identifiable information, or information that identifies cyber or physical vulnerabilities and protective measures for critical infrastructure.

¹⁴ State of Michigan Legislature. House Bill 4973. [http://www.legislature.mi.gov/\(S\(2y2l35mh5kbziusiaqqpqc50\)\)/mileg.aspx?page=getObject&objectName=2017-HB-4973](http://www.legislature.mi.gov/(S(2y2l35mh5kbziusiaqqpqc50))/mileg.aspx?page=getObject&objectName=2017-HB-4973).



Cybersecurity Roles for State and Territory Energy Offices

State Energy Offices work on policy, programs and operations with varying emphases. Energy cybersecurity can be reinforced in all three areas and there are several different roles that State Energy Officials can play in the cybersecurity space, all of which are important. State Energy Offices headed by the Governor's Energy Policy Advisor, should consider policy, programs, and operations to develop a comprehensive approach and strategic plan that engages all key stakeholder. For State Energy Offices that may be less policy-oriented and more program-focused, addressing cybersecurity in program design and operations that rely on information technology (IT) should be considered.

Even if their programs do not have significant IT risks, State Energy Office directors should, at a minimum, be concerned about their internal cybersecurity. It is fundamentally important to ensure that the technology upon which all State Energy Offices rely is secure. Following an energy sector cyber incident, for example, State Energy Offices are likely to have some responsibility for consequence management and information-sharing. It is vital to determine the extent of State Energy Offices' and other agencies' roles and responsibility – and how to coordinate most effectively with other key players – **before** a cyber incident. Familiarity with basic internal cybersecurity operations is critical to ensure continuity of operations following a cyber-attack whether on government-owned servers or on state energy resources or infrastructure.

It is also critical to be aware of resources housed within the state that may be able to assist in a cyber incident. Several states (e.g. Michigan, Wisconsin, Washington, Maryland) have National Guards which maintain cyber capabilities and assets to respond to cyber incidents and assist with incident response in the public and private sectors. State fusion centers serve as the intelligence and information-sharing focal points for states. Fusion centers are physical, trusted convening locations state and local law enforcement, critical infrastructure owners and operators, and cybersecurity and IT subject matter experts, among others. Fusion centers function to prevent and mitigate criminal and terrorist activities, including cyberattacks. Generally, this means that in addition to mitigative and investigative actions, a fusion center will seek to ensure that the functions of all response entities are not at risk of being compromised. It is important to note that fusion centers and the National Guard vary significantly from state to state. Thus, it is important for state energy officials to be aware of the entry points, communication avenues, and established relationships with their state National Guard and fusion centers, as both provide critical functions and capabilities for cyber preparedness and response.

Having a fundamental understanding of the various cybersecurity roles and responsibilities among state entities can significantly reduce the time needed to develop or improve the cyber functions of the State Energy Office.

Seven Frequently Asked Questions to Help Energy Officials Determine Cybersecurity Roles:

NASEO has consulted many State Energy Offices that do not yet have defined cybersecurity responsibilities. The following FAQs may help guide which roles could be appropriate to adopt. For a thorough example of what states can do, see [NASEO's State Energy Cybersecurity Models Analysis: Michigan Cybersecurity Structures and Programs Profile](#).

❑ If my state already has an overall cybersecurity strategy or plan, what steps can my office take to ensure energy sector priorities are integrated?

- If a broader cybersecurity strategy exists, the state CIO, CISO, or homeland security agency are likely involved. As energy sector subject matter experts, State Energy Officials may be ideally positioned to advise on energy system and infrastructure risks that may not be apparent to other state agencies involved in cybersecurity. The first step will be to identify all existing efforts by government to improve cybersecurity in the energy sector, including any related efforts by the PUC, homeland security agency, state fusion center, or other agencies. For example, the National Association of Regulatory Utility Commissioners has prepared a paper titled "[Cybersecurity Strategy Development Guide](#)" which details a process for PUC cybersecurity strategy development. It provides a general structured approach with important steps that should be followed. Many of the recommendations found in the NARUC guidance are applicable to State Energy Offices as well. NASEO highly recommends reviewing the document to begin the planning process with state, federal, and private partners.
- For engagement outside of state entities, the State Energy Office view of cybersecurity is broad and must therefore adopt an inclusive portfolio of cybersecurity strategies to include regulated, non-regulated, and consumer-owned utilities (both electric and natural gas), liquid fuel distributors and producers, and renewables. Additionally, considerations for energy-interdependent and system-integrated critical infrastructure, such as water treatment facilities, microgrids at key government buildings, and significant petroleum facilities should also be included. State Energy Offices often play an important role as conveners, bringing together key energy stakeholders to identify opportunities and chart courses of action to the collective mutual benefit of all parties. This can be an important way to begin the conversation with energy sector stakeholders within the state.

❑ How do I find out if my state currently has a cyber-incident response plan?

- Visit [NGA's State Cyber Disruption Response Plans](#) page mentioned earlier.
- If yes, it is important to determine if the plan has granular detail on energy-specific responses and if state's ESF-12 lead is involved. While a State Energy Office will likely not be the lead agency during cyber incident response, they are important to include to provide energy sector context to the broader response, be aware of major energy sector stakeholder cybersecurity plans and assets and know which external partners are most appropriate to engage. If no, a State Energy Office should ensure that any future developments should have energy sector buy-in, including private sector engagement and discussions with appropriate federal entities.

❑ How can my office better integrate cybersecurity into our strategic longer-term energy planning and program administration?

- Cybersecurity precautions should be considered in long-term energy planning. It is important to maintain awareness of risks to cybersecurity, such as vendor and supply chain vulnerabilities in state-supported endeavors. Cybersecurity should be considered as part of overall strategic planning to reduce risk and enhance resiliency of programs that may have significant cyber equities (including cybersecurity provisions in grant and/or loan programs funded through the office). For example, third-party retailers can be potential vectors of attack so an energy efficiency program that relies on energy management systems should be encouraged to have appropriate standards of cybersecurity for projects that are funded or managed by the State Energy Offices. The best way to ensure long-term internal cybersecurity is to include provisions in State Energy Office policy.

❑ What resources should my office develop in order to inform the development of cybersecurity strategy and policy by the Governor or Legislature?

- There may be a clear role to support energy sector cybersecurity through policy, program, and other initiatives. These could be pursued through the development of a specific cybersecurity strategy, in an update to the energy assurance plan or as part of a broader state initiative. High-level energy sector cyber risk assessments, including critical infrastructure interdependency analysis, would be effective in conveying the criticality of energy sector cybersecurity to lawmakers or government executives.

❑ Does my office have full or partial responsibility for the state’s energy security and assurance plan (EAP)?

- Ownership of the state EAP varies from state to state, but the cyber threats should be included as part of the “all hazards” approach adopted by all comprehensive energy assurance plans. Since these plans have been written, cyber threats have only grown and become more complex. With greater awareness and understanding, states updating their energy assurance plans have the opportunity to address this evolving risk in greater depth. If not, the roles of the responsible agency and a summary of their mitigation activities and response plans should still be included in the energy assurance plan. State Energy Offices will need to determine who, if anyone, is designated as Energy Emergency Assurance Coordinators, and if the State Energy Office is designated as the lead, co-lead, or general support for ESF-12 under the National Response Framework.

❑ How can my office assist the state in addressing cyber threats within its continuity of operations plan and investments?

- State Energy Offices should meet with the organization that provides their agencies’ information technology services and support to review their cybersecurity approach. State Energy Offices should also be familiar with how and where its organization files, stores, and backs-up all records. Has the back-up data been tested to assure its data integrity? Is there the ability to use the back-ups to restore primary systems if attacked or destroyed? Is everything current and up to date? What are the plans for disaster recovery? Are there employee education programs for cybersecurity best practices available to staff?
- State Energy Offices may also want to review their state government or energy office business continuity plan(s). Identification of and contingencies for essential roles and functions is critical in ensuring that a State Energy Office can continue operations even if affected by a cyberattack. Review [US-CERT’s Ransomware Executive One-Pager and Technical Assistance](#) for more information.

❑ How can my office support energy sector cybersecurity workforce development?

- According to the U.S. Department of Energy, unfilled cybersecurity careers will reach over 1.5 million by the end of 2019.¹⁸ This number is projected to grow substantially within the following years. The energy sector, with its increasing complexity, importance, and interdependent relationship with other critical infrastructures will demand a much larger, innovative, and better-prepared workforce to prepare for and response to cyber threats. State Energy Offices can help facilitate workforce development in their states by engaging universities, state departments of education, and the private sector to develop incentive programs to meet the growing need.

¹⁸ <https://cyberforcecompetition.com/about/>

Developing an Energy Sector Cybersecurity Planning and Response Strategy

The process for developing a state cybersecurity strategy is akin to a normal emergency preparedness planning cycle, but with a few additional and unique considerations. State Energy Offices should act based on on-the-ground realities and regional considerations. In developing the cybersecurity plan, the Energy Office should craft strategies according to the state's specific threats, needs, and available resources. Procedurally, this is nearly identical to a standard planning cycle, where cyber threats are included in a comprehensive risk assessment and mitigative solutions are sought thereafter.

Under normal circumstances and established procedures, a State Energy Office will likely never be the lead entity on cyber incident response plan. Cyber incidents require the involvement of many entities, and State Energy Offices may be among those consulted for energy-specific subject matter expertise and understanding of the potential economic and human impacts of energy sector disruptions. If an incident escalates into a sustained cyber-attack or has significant impacts, the response will require the involvement of additional entities and factors. The sensitivities around cyber-attacks need to be understood, as do the mechanisms for communicating critical information during cyber-incidents.

In their role(s) advising lead agencies on energy sector cybersecurity planning and incident response, it is also important for Energy Officials to be familiar with the [NCIRP](#),¹⁹ the federal government's framework for responding to cyberattacks. Working knowledge of federal responses will help states to develop and execute an effective overall cybersecurity strategy.

It is also helpful for State Energy Officials to know about recognized entities, mechanisms, policies, and procedures dedicated to cybersecurity at the state level. Such examples can serve as frameworks and best practices for states looking to develop their internal, external, and operational cybersecurity capacities.

¹⁹ https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Actions States and Territories Can Take to Improve Energy System Cybersecurity Risk Mitigation and Preparedness

State Energy Offices should take actions pursuant to their determined cybersecurity strategy, authorities, and responsibilities. resources, and other unique factors in each state should be accounted for when determining realistic, effective actions to enhance the ability to prepare for and respond to cyber incidents impacting the energy sector. The following is a list of some, but not all, actions a state should pursue in energy assurance planning and other cybersecurity planning efforts:²⁰

This section will explore three basic and potential roles that exist for State Energy Offices in cybersecurity policy development, stakeholder coordination, and incident response:

1. Supporting cyber risk mitigation and resiliency;
2. Assuring coordination across the public and private sectors; and
3. Responding to a cyberattack by managing consequences as part of all-hazards energy assurance/security planning and preparedness processes.

RISK MITIGATION AND RESILIENCY

POLICY

- Identify state authorities and legislative actions that can help improve cybersecurity. The [National Conference of State Legislatures \(NCSL\) tracks state legislation as it pertains to cybersecurity](#), though not all legislation pertains directly or broadly to energy security
- Consider cybersecurity as part of state's strategic energy plan
- Review your state's required notification laws and requirements related to cyber incidents or attacks on energy suppliers

PROGRAMS

- Include language in grants and contracts to enhance cybersecurity in the operation of state energy programs and other initiatives
- Drive the next generation of energy cybersecurity professionals by encouraging university students in your state to participate in CESER's annual, hands-on [Cyber force Competition](#)
- Review Best Practice Case Studies and explore the SLTT Toolkit on the [CISA Website](#)
- Determine if your office has any responsibility overseeing or inspecting pipeline safety and underground natural gas storage programs. In several states, this responsibility may fall to the PUC, but State Energy Offices might nonetheless find it useful to understand cybersecurity efforts in the pipeline sector

OPERATIONS

- Determine if there is any standard language in state procurement contracts that deal with cybersecurity and supply chain cybersecurity, and ensure it is sufficiently robust
- Assure that adequate disaster recovery and system backups are in place and tested. (These are the data systems upon which State Energy Offices rely and carry out their day-to-day functions. To ensure against loss of data and functional capabilities used by the agency, continuity of government operations plans need to be in place for essential functions)
- Examine and evaluate agency website and database security

²⁰ National Association of State Energy Officials. Assurance Guidelines Version 3.1. December 2009.

- ❑ Designate one or more staff as a cyber lead with responsibility for tracking cybersecurity matters, remaining current on state and federal efforts, and serving as a liaison to the private sector
- ❑ Work with other relevant state agencies and publicly owned utilities to provide cybersecurity education to local communities and governments. Topics could include basic cyber hygiene and the benefits of cybersecurity investments in utility infrastructure

COORDINATION

POLICY

- ❑ Engage and support the private energy sector in their efforts to improve cybersecurity
- ❑ Support the [Energy Emergency Assurance Coordinator Agreement](#) signed by NASEO, NGA, NARUC, National Emergency Management Association (NEMA) and the U.S. Department of Energy

PROGRAMS

- ❑ Consider using your office's non-regulatory convening power (an option in many, but not all, states) to bring together various private and consumer-owned energy providers to discuss non-sensitive cyber security actions they are taking, encourage cooperation with relevant federal and state entities, and identify needs to communicate to your governor and legislature
- ❑ Join your local [InfraGard](#) chapter to become part of a vetted public-private information-sharing network dedicated to protecting critical infrastructure. This provides states with another information sharing mechanism and builds relationship with other private sector members who are also concerned about cybersecurity
- ❑ Contact your state's Bureau of Investigation's Cybersecurity group to become familiar with staff, services, and key points of contact
- ❑ Become a member of the [Multi State-ISAC \(MS-ISAC\)](#)
- ❑ Work with your [state Fusion Center](#) to potentially receive information on threats to your critical energy

OPERATIONS

- ❑ Develop relationships with organizations that support cybersecurity. This could include: the state's chief information officer; PUC cybersecurity activities; EnergySec; the SANS Institute; the Federal Bureau of Investigation's InfraGard program; the Multi-State Information Sharing and Analysis Center (ISAC); state fusion centers; electric, oil and natural gas, and downstream natural gas ISACs, etc.
- ❑ Get to know the state's designated regional Protective Security Advisor (PSA) [by contacting CISA directly](#)
- ❑ [Contact a Cyber Security Advisor \(CSA\)](#) within CISA's Infrastructure Security Division (ISD)
- ❑ Contact your DHS [Regional Office](#) to learn about regional training, risk mitigation, and coordination opportunities
- ❑ Assure communication and information sharing channels internal to state Government are clear and defined in the event of an energy disruption or new significant threat
- ❑ Assure that public communication and information sharing channels are clear and defined when an incident occurs
- ❑ Inform states in your region of actions taken by your state in response to an energy supply disruption as provided for in the Energy Emergency Assurance Coordinator agreement

ENERGY EMERGENCY RESPONSE PLANNING

POLICY

- Engage other government agencies that have a role in an energy sector cyber incident response that may be broader than just the energy sector
- Understand what actions are being undertaken by state government and the public and private energy sectors to promote cybersecurity
- Update all state, local and regional energy emergency contacts in the public and private sectors annually

PROGRAMS

- Consider participating in or hosting a cybersecurity incident response exercise or workshop to test existing emergency plans, define roles and responsibilities, and identify planning gaps
- Test the state's capabilities and plans by playing in CESER's energy sector cybersecurity exercises. Email exercises@hq.doe.gov to join the Energy Sector Exercises Quarterly Forum webinar and learn about upcoming CESER, other federal agency, and industry exercises
- During "blue sky days," collaborate with private sector partners to share information on priority critical infrastructure and facilities in order to sort through potential restoration discrepancies, identify interdependencies, and assure that the energy supply or backup power function is cyber-secure
- Register for and participate in the NERC/E-ISAC bi-annual [Grid Security Exercise \(GridEx\)](#)
- Conduct training for state officials new to energy emergency response activities
- Participate in DOE CESER's Energy Emergency Response Training (available in late 2020)
- Include cybersecurity contingencies and messaging templates in your office's or state's Public Information Program

OPERATIONS

- In the event of a cyber incident, ensure you contact the FBI, DHS CISA, and/or DOE CESER
- Print and distribute plans and updated contact lists for offline reference and manual operation
- Assure that energy assurance/security plans are up to date and address cybersecurity and clearly define state agency roles and responsibilities
- Identify the primary and secondary points of contact from the State Energy Office and PUC (or other relevant agencies) and those that are designated as the state [Energy Emergency Assurance Coordinator \(EEAC\)](#). It is up to each state to designate who will serve as the EEAC. DOE/CESER and NASEO can provide information on state contacts
- Register for [EAGLE-I](#), the interactive geographic information system used to view and map energy infrastructure and obtain near real-time visual updates concerning the electric, petroleum, and natural gas sectors
- Register for access to [DHS' Infrastructure Protection \(IP\) Gateway](#), which provides various data collection, analysis, and response tools to SLTT governments on a verified need-to-know basis for qualifying and vetted applicants. Contact the IP Gateway Help Desk [here](#) to get started
- Request a nomination for access to the Homeland Security Information Network (HSIN) by contacting CESER/ISER or NASEO

Disclaimer: This action list is not exhaustive. Each State Energy Office will have unique factors that may determine which actions are necessary and feasible. NASEO, in partnership with DOE CESER, can help State Energy Offices determine their roles, develop their cybersecurity strategy, and execute the actions which will help increase state cybersecurity and ensure that the energy sector is properly postured to mitigate cyber threats and respond to cyber incidents.



Afterword

Cyber threats to energy infrastructure integrity and functionality are persistent and evolving. Energy sector cybersecurity requires all stakeholders to be aware of and involved in ongoing efforts to protective, preventative, and mitigate risks. Single vulnerabilities can jeopardize entire systems and put human and economic health and security at risk. Through growing complexities and nuances, government and industry must continue to build mutually beneficial relationships, share information, and jointly prepare and respond to ensure the highest possible level of cybersecurity. In 2017, the NASEO Board of Directors passed a [Resolution on Energy Emergency and Cyber Security Planning, Preparedness, and Response](#), which has since served as the guiding internal doctrine for NASEO's cybersecurity activities.

NASEO will be involved in the following near-term cybersecurity activities:

- Contribute to a Cybersecurity Information-Sharing Paper (Collaboration with NARUC and NGA);
- Complete a Cyber Workforce Development Paper;
- Provide updated guidance for a Cybersecurity for Energy Assurance Planning; and
- Support various Cyber Incident Response Exercises.

Through its Energy Security Committee and partnerships with DOE CESER, NARUC, NGA, NEMA, NCSL, industry trades, and others, NASEO will continue to ensure that State Energy Offices are able to perform their steady-state and emergency response duties even in the event of an internal cybersecurity compromise, and that they are able to adequately and effectively plan for and respond to cybersecurity incidents affecting the energy sector.

Annex A: Federal Policy and Guidance

Policy	Year Issued	Description
Presidential Decision Directive 63 – Critical Infrastructure Protection	1998	Initial federal executive branch strategy intended to eradicate significant physical and cyber vulnerabilities on the nation’s critical infrastructures. Designated DOE as the federal lead for the energy sector. Set the stage for the creation of Information Sharing and Analysis Centers (ISAC) for each critical infrastructure sector.
Energy Policy Act of 2005	2005	Designated FERC as federal entity responsible with reliability of the electric grid.
Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience	2013	Directed the federal government to work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the nation’s critical infrastructure. Designated DOE as the sector-specific agency for critical infrastructure.
Executive Order 13636: Improving Critical Infrastructure Cybersecurity	2013	Directed the executive branch to promote and incentivize cybersecurity information-sharing, privacy protections, and adoption of cyber-minded practices and frameworks.
Fixing America’s Surface Transportation (FAST) Act	2015	Designated DOE as the Sector-Specific Agency for Energy Sector Cybersecurity. Provides authorities to the Secretary of Energy to order emergency measures, following a Presidential declaration of a grid security emergency (GSE), to protect or restore the reliability of critical electric infrastructure or defense critical electric infrastructure during the emergency. A cyber-attack could initiate a GSE.
Presidential Policy Directive 41—United States Cyber Incident Response Coordination	2016	Outlined the guiding principles for coordinated cyber incident coordination and response and acknowledged the roles and responsibilities that states have during a significant cyber incident.
National Cyber Incident Response Plan (NCIRP)	2016	Primary strategic framework for stakeholders to understand how the various federal departments and agencies and other national-level partners provide resources to support response operations.
Presidential Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	2017	Required an assessment of the potential scope and duration of a prolonged power outage caused by a significant cyber incident.
DOE Multiyear Plan for Energy Sector Cybersecurity	2018	Set objectives for DOE regarding energy sector preparedness, response, recovery, research and development
Cybersecurity and Infrastructure Security Agency Act of 2018	2018	Designated the National Protection and Programs Directorate of U.S. DHS as the Cybersecurity and Infrastructure Security Agency, with expanded cybersecurity roles and responsibilities
National Cyber Strategy of the United States	2018	Clarified federal government’s commitment to cybersecurity, including securing critical infrastructure with priority risk mitigation actions, investment incentives, and research and development investments.