NATIONAL GOVERNORS ASSOCIATION

ENERGY CYBERSECURITY RESOURCES FOR GOVERNORS' ADVISORS

Background and Regulatory Authority

As malicious actors increasingly target energy infrastructure with cyber-attacks, it's important that Governors' advisors understand the risks to energy infrastructure in their states and territories, and the roles state and territory leaders can play to address those risks. A cyber-attack on critical infrastructure in the United States, including on energy infrastructure, poses a significant threat and could cause major disruptions to day-to-day life, endanger public safety and health, and result in millions of dollars in economic losses. In May of 2021, a ransomware attack on the information technology (IT) systems of the Colonial Pipeline led operators to shut down the pipeline for multiple days out of an abundance of caution, resulting in fuel shortages and consumer panic.

In 2023, President Biden released the National Cybersecurity Strategy to establish a framework to protect critical infrastructure from cyberattacks. In addition, President Biden penned a letter to governors encouraging the adoption of state cybersecurity standards to protect critical energy infrastructure. As the leaders of their states, Governors are ultimately responsible for preparing for and responding to energy emergencies. Governors can defend critical infrastructure from cyber threats by taking a proactive approach to assess cybersecurity resilience, identify gaps, and plan for emergencies. The purpose of this resource guide is to provide an overview of federal and state cybersecurity standards for the energy sector as well as a collection of energy cybersecurity resources from the National Governors Association (NGA), the federal government, and other state focused organizations.

Electric Sector

Federal Standards

Cybersecurity standards for the bulk power system in the United States are governed by the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Reliability Standards. NERC is a not-for-profit international regulatory authority whose mission is to "assure the effective and efficient reduction of risks to the reliability and security of the grid." Its standards are enforced in the United States and Canada; portions of Mexico have also adopted NERC standards. In the U.S., NERC derives its authority from the Federal Energy Regulatory Commission (FERC) as the designated Electric Reliability Organization tasked with developing and enforcing mandatory reliability standards. Cybersecurity is covered under NERC's CIP Reliability Standards. NERC CIP Standards are separated into several topic areas, detailed below. NERC performs periodic audits of grid operators and can levy financial fines for non-compliance. The NERC CIP standards ensure a minimum level of cybersecurity best practices are maintained.

NERC CIP Mandatory Enforced Standards:

- CIP-002-5.1a Bulk Electric System (BES) Cyber System Categorization
- CIP-003-8 Security Management Controls
- CIP-004-6 Personnel & Training
- CIP-005-7 Electronic Security Perimeter(s)
- CIP-006-6 Physical Security of BES Cyber Systems
- CIP-007-6 System Security Management
- CIP-008-6 Incident Reporting and Response Planning
- CIP-009-6 Recovery Plans for BES Cyber Systems
- CIP-010-4 Configuration Change Management and Vulnerability Assessments
- CIP-011-2 Information Protection
- CIP-012-1 Communications between Control Centers
- CIP-013-2 Supply Chain Risk Management
- CIP-014-3 Physical Security

State-level Authorities

While few states maintain cybersecurity standards for the distribution system, those that are in place are typically overseen by the public utility commission (PUC). Public utility commissions regulate the rates and services of electric and gas utilities, which also includes jurisdiction over reliability from physical and cyber events. Authorities vary from state to state but most Commissions have authority to review the cybersecurity practices of utilities under their jurisdiction and compel utilities to disclose major cyber breaches that have an impact on meeting electricity demand.

Many public power utilities and rural electric cooperatives are outside of regulatory oversight of states and NERC, and therefore subject to self-regulation. The degree to which they can be regulated by states varies state-by-state. A 2017 study by the National Renewable Energy Laboratory found that the cybersecurity capacity of these smaller utilities varies, with some lacking the resources to facilitate a robust cybersecurity program. In 2022, President Biden penned a letter to Governors encouraging the adoption of state cybersecurity standards for critical energy infrastructure. On behalf of the Council of Governors, **Minnesota** Governor Tim Walz and **Ohio** Governor Mike DeWine reinforced the importance of cybersecure energy infrastructure and a whole-of-government approach to cybersecurity in a May 4, 2022 response to the President. The letter recommended a consistent, federally-coordinated approach to cyber standards for the energy sector.

Recognizing the importance of a standardized approach to cybersecurity standards, DOE CESER is currently working with the National Association of Regulatory Utility Commissioners (NARUC) to "establish a set of cybersecurity baselines that states can consider and adopt for distribution systems and distributed energy resources."

Pipeline Owners and Operators

Federal Standards

On the federal level, cybersecurity standards for pipeline owners and operators are overseen by the Department of Homeland Security Transportation Security Administration (TSA). Prior to the Colonial Pipeline attack, TSA advocated voluntary pipeline cybersecurity standards for two decades. Initial mandatory cybersecurity rules for owners and operators of pipelines were issued in July of 2021 and were updated on July 21, 2022. The 2022 security directive has been deemed sensitive and is not available to the public, but builds upon the initial 2021 directive which requires pipeline owners to:

- Report confirmed or potential cybersecurity incidents to CISA,
- Designate a Cybersecurity Coordinator to be available 24 hours a day, 7 days a week,
- Review current cybersecurity practices, and
- Identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days.

Resources

Opportunities for Cybersecurity Investment in the Bipartisan Infrastructure Investment and Jobs Act (IIJA)

This commentary, published by NGA in 2022, discusses the opportunities for states to invest in cybersecurity using funding in the Bipartisan Infrastructure Investment and Jobs Act (IIJA) passed into law in 2021. The IIJA contains about $1.2 trillion in funding towards nearly 400 new and existing infrastructure programs and includes a number of cybersecurity-specific programs, as well as allowing spending from numerous other programs on cybersecurity preparedness and response, which can be integrated into other infrastructure investments.

NGA Center Energy Cybersecurity Resources

- **States' Role in Addressing Foreign Threats in U.S. Critical Energy Infrastructure Sectors (2022)**
  This issue brief examines the vulnerabilities of critical energy infrastructure sectors and assets to foreign threats and identifies possible actions Governors can take to address those vulnerabilities. Critical energy infrastructure systems, including electric power, natural gas, and petroleum, are the backbone of all other critical infrastructure systems, meaning that an energy supply failure triggered by a cyber-attack could have cascading effects on transportation, water, telecommunications, finance, healthcare and other sectors.
- **Addressing Cybersecurity for Critical Energy Infrastructure through State Governing Bodies (2021)**
  This paper reviewed eight state efforts to address cybersecurity vulnerabilities of critical energy infrastructure by establishing effective statewide cybersecurity governance bodies.
- **State Energy Toolkit: Addressing Cyber and Physical Threats (2019)**
  The toolkit offers ideas to help Governors respond to trends as they act in their states to address cyber and physical threats. The guide includes an overview of the technologies and key policy trends; a summary of opportunities, challenges, and key state solutions; and a menu of state policy solutions, spotlighting examples from leading states.
- **State Protection of Critical Energy Infrastructure Information (2019)**
  This policy scan explores state laws that protect critical energy infrastructure information (CEII) from public disclosure. It also addresses court rulings protecting sensitive data for other infrastructure types and explores how states are protecting shared critical data from cyberattacks and cyber theft.

- **Smart & Safe: State Strategies for Enhancing Cybersecurity in the Electric Sector (2019)**
  This white paper outlines seven actions governors can take in order to protect electricity infrastructure and personally identifiable information from cyberattacks. The paper also details roles and responsibilities for key state, industry and federal entities and catalogues important resources.

External Energy Cybersecurity Resources for States

- **APPA** Cybersecurity Resource Guide for Public Power Utilities – This report provides a high-level guide for cybersecurity protections for the critical infrastructure systems and digital assets of public power utilities.
- **NASEO** Enhancing Energy Sector Cybersecurity – Pathways for State and Territory Energy Offices (2020) – This report provides background on ongoing cybersecurity efforts in both the public and private sectors and identifies state-relevant communication channels and mechanisms for sharing information. Additionally, it identifies roles State and Territory Energy Offices might play in enhancing cybersecurity and response actions.
- **NASEO/NARUC** Cybersecurity Advisory Team for State Solar Webpage & Resources – This project jointly led by NASEO and NARUC intends to mitigate cybersecurity risks solar energy developments and leverages state, federal, and private-sector expertise to identify model solar-cybersecurity programs and actions for states to take in partnership with utilities and the solar industry.
- **NARUC** Compendium of Cyber Incident Notification Requirements for Critical Infrastructure Utilities by State (2022) – This compendium identifies state requirements for private businesses, including energy utilities, to notify individuals of cybersecurity breaches of information involving personally identifiable information (PII).
- **NARUC** A Guide for PUCs: Recruiting and Maintaining a Cybersecurity Workforce (2021) – This reference guide describes the role of cybersecurity personnel within a PUC and a range of cybersecurity skill sets that may fit a PUC's needs, as well as avenues for recruiting, retaining, and growing cybersecurity expertise. Appendices provide lists of cybersecurity training resources, recruitment pipelines, and a compendium of sample cybersecurity job descriptions.
- **NARUC** Cybersecurity for the Smart Grid: Questions for Utilities (2020) – This paper introduces cybersecurity topics relevant to the smart grid and suggests questions PUCs might ask of utilities to better understand how they are assessing and mitigating these cyber risks to digitized systems.
- **NARUC** Cybersecurity Primer for State Utility Regulators: Version 3.0 (2017) – This primer presents an overview of the cybersecurity landscape, highlights best practices for cybersecurity, and offers recommendations for state utility regulators to develop a cybersecurity strategy.
- **NARUC** Risk Management in Critical Infrastructure Protection: An Introduction for State Utility Regulators (2016) – This paper introduces strategies for risk management and discusses strategies state utility regulators can employ to manage risks to critical infrastructure.
- **NARUC** Cybersecurity Manual
  - Cybersecurity Strategy Development Guide
  - Cybersecurity Preparedness: Questions for Utilities
  - Cybersecurity Preparedness Evaluation Tool
  - Cybersecurity Tabletop Exercise Guide
  - Cybersecurity Glossary

- **NCSL** 2021-2022 Energy Security State Legislative Review: Cybersecurity and Physical Security (2022) – This report outlines relevant state legislation considered and/or enacted in 2021 and 2022 that aimed to bolster the security of states' energy infrastructure against physical and cyber threats.
- **NCSL** Cybersecurity and the Electric Grid – The state role in protecting critical infrastructure (2020) – This paper provides an overview of the regulatory role states, particularly state legislatures, can play in establishing cybersecurity protections and standards for critical infrastructure, including energy assets.
- **NEMA** Best Practices for Energy Resilience and Cybersecurity: The Role of State Emergency Management Agencies (2023) – This guide discusses the critical role of state emergency management agencies in responding to energy emergencies and provides resources and best practices for emergency managers on cybersecurity and energy resilience.
- **NEMA** Guiding Principles for Emergency Management on Cybersecurity (2020) – This document outlines guiding principles for emergency management executives around cybersecurity.

Federal and Industry Websites and Resources

- **White House** 2023 National Cybersecurity Strategy **–** Biden-Harris Administration cybersecurity framework to protect critical infrastructure, disrupt threat actors, shape market forces to promote security, make investments in cybersecurity research and development, and create international cybersecurity partnerships.
- **Department of Energy (DOE) – Cybersecurity, Energy Security, and Emergency Response Office (CESER)**
  - National Cyber-Informed Engineering Strategy (2022) – This paper outlines the Department of Energy's cyber-informed engineering (CIE) strategy to mitigate cyber risks across the lifecycle of devices and systems in critical energy infrastructure.
  - State Energy Security Plan Optional Drop-In: IT/OT and Cyber Threat Overview (2022) – This document provides relevant information on cybersecurity for informational technology (IT) and operational technology (OT) systems for states updating their energy security plans.
  - Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid (2022) – This report provides an overview of cybersecurity considerations that should be considered by the electric sector, including utilities and distributed energy resources (DER) operators, providers, integrators, developers, and vendors, as well as policymakers.
  - Cybersecurity Capability Maturity Model (2022) **–** The Cybersecurity Capability Maturity Model (C2M2) is a free tool developed by DOE CESER to help organizations evaluate their cybersecurity capabilities.
  - CyberForce Program – The Department of Energy facilitates the CyberForce program to bolster the energy cybersecurity workforce.
  - Energy Waiver Library – Compiled resource of federal waivers and other regulatory relief available to states to expedite restoration of affected energy systems during emergencies.
  - State, Local, Territorial, and Tribal Program Resource Library – The DOE CESER SLTT library provides resources to advance state, local, tribal, and territorial government's energy security planning, risk awareness, policy and investment decisions, mitigation strategies and emergency response efforts.

- **Department of Homeland Security – Cybersecurity Infrastructure Security Agency (CISA)**
  - CISA Cross-Sector Cybersecurity Performance Goals (CPGs) – The CISA CPGs are a subset of voluntary cybersecurity practices, selected through a process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people.
  - Cyber Incident Resource Guide for Governors – This guide provides information for governors and their staff on how to request federal support during or following a cyber incident.
  - Energy Sector Webpage
  - Energy Sector-Specific Plan for Infrastructure Protection (2015)
  - Energy Sector: Council Charters and Membership
- **GridEx –** A national grid exercise hosted by the NERC Electricity Information Sharing and Analysis Center (E-ISAC) and supported by NGA that simulates a cyber and physical attack on the North American electricity grid and other critical infrastructure. GridEx engages both the public and private sectors and allows NERC and the E-ISAC to consolidate best practices and lessons learned from the exercise in a follow-up report.
- **National Institute for Standards and Technology (NIST) National Cybersecurity Center of Excellence**
  - Energy Resources Webpage
  - Trustworthy & Responsible AI Resource Center
- **Electricity Subsector Coordinating Council**
  - Cyber Mutual Assistance
- **Oil-Natural Gas Subsector Coordinating Council**
  - ONG Cybersecurity 101
  - Defense-In-Depth: Cybersecurity in the Natural Gas & Oil Industry Report
- **National Council on Electricity Policy**
  - State Agency Coordination During Energy-Related Emergencies Guide

Technical Assistance

The NGA Center for Best Practices will continue to track key energy cybersecurity trends and updates for Governors and their advisors. As this field continues to evolve, NGA Center staff are available to respond to quick turnaround technical assistance requests through policy memos or connections with experts to answer urgent questions. For any energy security, emergency preparedness and cybersecurity technical assistance requests, please contact Dan Lauf (dlauf@nga.org), Jessica Davenport (jdavenport@nga.org), or Steve Fugelsang (sfugelang@nga.org).

This material is based upon work supported by the Department of Energy, Office of Electricity under Award Number DE-CR0000011.