ENERGY CYBERSECURITY RESOURCES FOR GOVERNORS' ADVISORS

Background

On the federal level, cybersecurity standards in the United States are governed by the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Reliability Standards. NERC's mission is to "ensure the reliability of the North American bulk power system". Their standards are enforced in the United States and Canada; portions of Mexico have also adopted NERC standards. In the U.S., NERC derives their authority from the Federal Energy Regulatory Commission (FERC) since they are 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.

CIP-002-5.1a	BES Cyber System Categorization
CIP-003-8	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-6	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-010-3	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection
CIP-013-1	Supply Chain Risk Management
CIP-014-2	Physical Security

On the state level, energy cybersecurity standards are usually overseen by the state 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.

NGA Center Energy Cybersecurity Resources

- **State Energy Toolkit: Addressing Cyber and Physical Threats**
  The toolkit offers ideas to help governors respond to trends as they take action in their states in addressing 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**
  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 Security**
  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 State Energy Resources

- **NASEO Enhancing Energy Sector Cybersecurity – Pathways for State and Territory Energy Offices**

- **NARUC Cybersecurity Primer for State Utility Regulators: Version 3.0**

- **NARUC Risk Management in Critical Infrastructure Protection: An Introduction for State Utility Regulators**

- **NARUC Case Study: Public Utility Participation in GridEx V**

- **NARUC Cybersecurity Manual**
  - **Cybersecurity Strategy Development Guide**
  - **Cybersecurity Preparedness: Questions for Utilities**
  - **Cybersecurity Preparedness Evaluation Tool**
  - **Cybersecurity Tabletop Exercise Guide**
  - **Cybersecurity Glossary**

Useful Industry Websites and Resources

Department of Energy – Cybersecurity, Energy Security, and Emergency Response Office (CESER)
https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response

Department of Homeland Security – Cybersecurity & Infrastructure Security Agency (CISA)
https://www.cisa.gov/cybersecurity

NERC CIP Reliability Standards
https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Electricity Subsector Coordinating Council Cyber Mutual Assistance
https://www.electricitysubsector.org/en/CMA

Defense-in-Depth: Cybersecurity in the Natural Gas & Oil Industry
http://naturalgascouncil.org/wp-content/uploads/2018/10/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf

Edison Electric Institute – National Security Efforts in the Electric Power Sector
https://www.eei.org/issuesandpolicy/Documents/national_security_efforts_in_the_electric_power_sector.pdf

American Public Power Association Cybersecurity Resources
https://www.publicpower.org/topic/cybersecurity-and-physical-security

GridEx – A national grid exercise that simulates a cyber and physical attack on the North American electricity grid and other critical infrastructure.
https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx

Liberty Eclipse - Regional energy assurance exercise from the Department of Energy to promote state- and local-level preparedness and resilience for future energy emergencies stemming from a cyber incident.
https://www.energy.gov/ceser/emergency-response/exercises-and-training

Technical Assistance

The NGA Center 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 assurance and cybersecurity technical assistance requests, please contact Alyse Taylor-Anyikire at atanyikire@nga.org.***