NARUC
National Association of Regulatory Utility Commissioners

ACCESS THIS GUIDE VIRTUALLY

# Essential Guide to NARUC Cybersecurity Resources

## Overview

National Association of Regulatory Utility Commissioners (NARUC) members are increasingly seeking more information about cybersecurity infrastructure needs, impacts, and the role of public utility commissions (PUCs). This guide connects commissioners and commission staff to essential cybersecurity resources that NARUC has developed. All of these resources can be found on the NARUC Cybersecurity webpage.

The NARUC Center for Partnerships & Innovation (CPI) works to provide state utility regulators with strategies, tools, and expertise to engage utilities in discussions about cybersecurity preparedness, response, and recovery planning, policies, and practices. These initiatives, coupled with training and technical assistance, support PUCs in their mission to ensure safe, reliable, and resilient energy infrastructure at reasonable rates. For more information, contact Lynn Costantini, lcostantini@naruc.org.

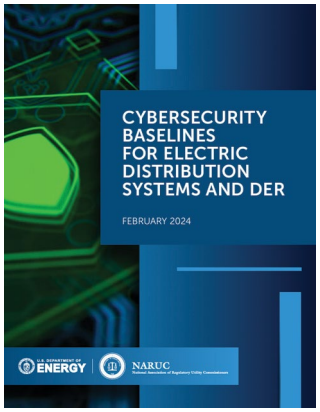
## Foundational NARUC Resources on Cybersecurity and the Role of PUCs

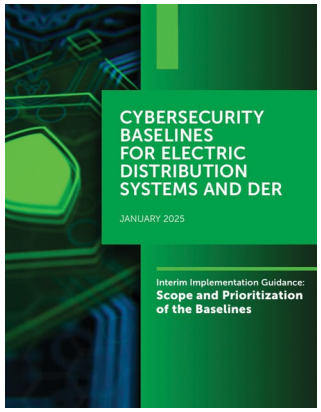
The resources below provide a starting point for further exploration of cybersecurity.

- Cybersecurity Baselines for Electric Distribution Systems and DER

  NARUC, in partnership with the U.S. Department of Energy (DOE), Office of Cybersecurity, Energy Security, and Emergency Response (CESER), has developed cybersecurity baselines for electric distribution systems and distributed energy resources to enhance grid security. These guidelines, informed by a diverse group of experts, aim to help state commissions, utilities, and DER operators align their cybersecurity practices and mitigate risks.

  - The Cybersecurity Baselines
  - Implementation Guidance




### About the NARUC Center for Partnerships & Innovation

NARUC CPI identifies emerging challenges and connects state commissions with expertise and strategies to navigate their complex decision-making. CPI accomplishes this goal by building relationships, developing resources, and delivering training that provides answers to state commissions' questions.

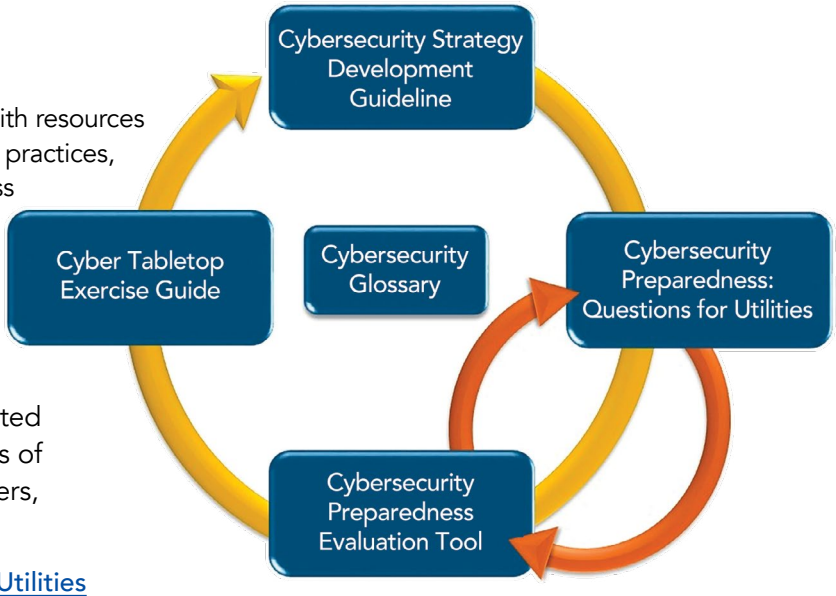
NARUC CPI conducts work in five key energy topics: generation; transmission; distribution; customers; and critical infrastructure, cybersecurity, and resilience. Find all resources and upcoming events at: www.naruc.org/cpi.

- Cybersecurity Manual

  NARUC's Cybersecurity Manual provides PUCs with resources to assess utilities' cybersecurity risk management practices, enabling informed decisions on their effectiveness and related expenditures. Within this resource are critical tools for regulators, such as:

  - Cybersecurity Strategy Development Guide

    This document aims to guide commissions' interactions with their utilities on issues related cybersecurity, drawing from the experiences of federal, state, and private-sector stakeholders, including state PUCs themselves.




  - Cybersecurity Preparedness: Questions for Utilities

    This resource provides a set of comprehensive, context-sensitive questions that PUCs can ask of a utility to gain a detailed understanding of its current cybersecurity risk management program and practices. The questions build upon and add to those included in prior NARUC publications.

  - Cybersecurity Preparedness Evaluation Tool

    The CPET provides a structured approach for PUCs to use in assessing the maturity of a utility's cybersecurity risk management program and gauging capability improvements over time. The CPET is designed to be used with the *Questions for Utilities* on an iterative basis to help PUCs identify cybersecurity gaps, spur utilities' adoption of additional mitigation strategies, and inform cybersecurity investment decisions.

  - Cybersecurity Tabletop Excercise Guide

    This guide details the steps that PUCs can take to design, execute, and evaluate a cybersecurity-focused tabletop exercise. An exercise could examine utilities' and other stakeholders' readiness to respond to and recover from a cybersecurity incident or analyze the PUC's internal capabilities.

  - Cybersecurity Glossary

    This glossary contains cybersecurity terms used throughout the Cybersecurity Manual, as well as "terms of art" that utilities may use during discussions with PUCs. It also includes a list of cybersecurity related events that demonstrate the growing threats and vulnerabilities against critical infrastructure sectors.

### Trainings and Experiential Learning

- **Cybersecurity Training for Regulators**, Fall 2025

  NARUC conducts in-person training events that focus on cybersecurity topics through the lens of a public utility regulator. Subject matter experts, recruited from around the country, make presentations, lead discussions, and offer topical and timely "boots on the ground" perspectives. **The next training will take place October 15 to 17, 2025, in Nashville, TN. Find details and registration on the** NARUC Cybersecurity webpage.

- On-Demand Cybersecurity Training Modules

  DOE CESER, in partnership with NARUC, have produced a set of on-demand cybersecurity training modules. Much of the content included in the training is based on NARUC's *Cybersecurity Manual*. These comprehensive training resources, which take approximately six hours to complete, are designed to empower participants with the necessary skills and knowledge to navigate the dynamically evolving landscape of utility regulation while ensuring robust cybersecurity preparedness.

## Publications and Activities on Key Cybersecurity Topics

The following resources can be found on the NARUC Cybersecurity webpage. Hyperlinks lead to PDFs of the publications or webinar presentations. To view recordings of past webinars, visit the Cybersecurity webpage or NARUC's YouTube channel.

### Coordination, Staffing, and Reporting for Cybersecurity

- Fusion Centers and State Energy Stakeholders: Pathways to Robust Threat Information Sharing, Fall 2023

  This mini guide explores the current landscape of threat information sharing between fusion centers and state energy stakeholders. Based on interviews with a sampling of key stakeholders, from PUCs, State Energy Offices, state offices of emergency management, and fusion centers, the mini guide highlights areas of successful practice, current challenges, and opportunities for potential improvements.

- Compendium of Cyber Incident Notification Requirements for Critical Infrastructure Utilities by State, July 2022

  This resource details state-by-state requirements for utilities to report cybersecurity incidents. Links to statutes and orders are included.

- A Guide for Public Utility Commissions: Recruiting and Retaining a Cybersecurity Workforce, February 2021

  This paper serves as a reference guide for PUCs trying to develop or expand their cybersecurity proficiency. It 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 for PUC consideration.

- Cybersecurity for the Smart Grid: Questions for Utilities, December 2020

  This paper introduces cybersecurity topics relevant to the smart grid. It also suggests questions PUCs might ask utilities to better understand how they are assessing and mitigating the new risks associated with advancing technologies that comprise the smart grid. Concepts in this paper draw from seminal works by the National Institute of Standards and Technology (NIST) as well as topics introduced in NARUC's Cybersecurity Manual. This paper is a complement to *Understanding Cybersecurity Preparedness: Questions for Utilities*.

### Emerging Issues

- Tech Talk for Regulators Episode One: The Intersection of Artificial Intelligence and Cybersecurity, April 2024

  During this podcast episode, subject matter experts explore the risks and rewards of using AI to enhance utilities' cybersecurity posture.

- Emerging Issues Brief: Volt Typhoon, February 2024

  This brief describes the threat to critical infrastructure posed by the cyber threat actor group known as Volt Typhoon. It contains questions PUCs may consider asking utilities about their actions to identify and mitigate malicious Volt Typhoon-related activity on their critical systems.

### Cybersecurity for Distributed Energy Resources (DER)

- Cybersecurity Advisory Team for State Solar (CATSS)

  Created by the National Association of State Energy Officials and NARUC, the CATSS Toolkit provides State Energy Offices and public utility commissions with actionable information on cybersecurity for solar power and supports state cybersecurity enhancements for solar and other distributed energy resources.

- CATSS Literature Review

  This literature review provides an overview of relevant reports and research on solar cybersecurity issues by categories including general cybersecurity resources, interconnection resources for DER, cybersecurity resources for DER, state examples, roadmaps, technical resources for vulnerability and threat assessment, and technical resources for potential solutions and frameworks.

- Webinar: Initiative on Cybersecurity in Solar Projects: Cybersecurity Advisory Team for State Solar (CATSS), April 2021

  This webinar explored the drivers accelerating solar adoption, the new cybersecurity risk landscape for solar and efforts underway to address the challenges, and the roles that state commissions and energy offices play in shaping the future of grid reliability, security, and resilience.

- Hypothetical Solar Cyberattacks Scenarios and Impacts

  This resource presents hypothetical risk scenarios illustrating how cyberattacks could affect solar PV systems and related infrastructure. It outlines potential consequences, types of attacks, and state-level actions to reduce risks, and is intended to support state regulators and state energy officials in understanding and planning for solar cybersecurity threats.

### International Best Practices in Cybersecurity

- The Utility Regulator's Role in Promoting Cybersecurity: Resilience, Risk Assessment, and Standards, April 2020

  This guide was initially developed for regulators in Europe and Eurasia to reinforce their knowledge of practical cybersecurity solutions in the face of ongoing threats within the energy sector. However, the questions of how to evaluate risks, assess mitigation measures, and select standards are relevant for regulators around the world.

- Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators, May 2020

  These guidelines were developed to assist regulators in ensuring that investments made in the name of cybersecurity are reasonable, prudent, and effective. They are intended to assist regulators in defining tariffs by establishing a regulatory approach to enhance the cybersecurity stance of their power systems and are based on literature and current practices.

- Understanding Cybersecurity Maturity Models within the Context of Energy Regulation, September 2020

  The goal of this primer is to provide an understanding of the fundamental principles of maturity models so that the greatest benefit can be realized from their use, rather than ranking maturity models against each other. This will permit regulators to work efficiently and effectively with utilities on cybersecurity regardless of the cybersecurity model that is selected for use, whether by the regulator or the utility.

### Non-NARUC Cybersecurity Resources

- NIST Cybersecurity Framework

  This framework offers voluntary guidance to help organizations understand and improve their management of cybersecurity risks.

- North American Electric Reliability Corporation's Reliability Standards

  These standards are collaboratively developed through an open, transparent, and consensus-driven process to define performance-based, risk-informed requirements for ensuring the reliable planning and operation of the North American bulk power system.

- ISO/IEC Information Security Controls for the Energy Utility Industry, 2024

  This document provides information security controls for the energy utility industry, based on ISO/IEC 27002:2022, for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes.