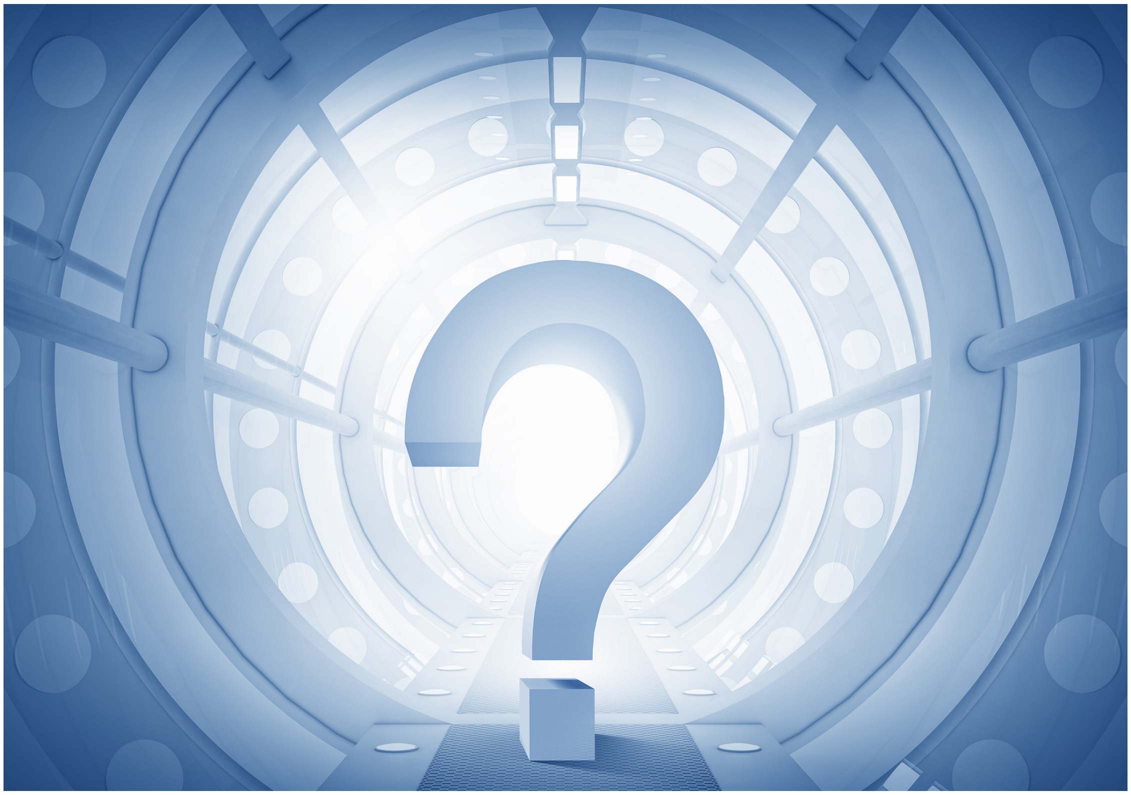
NARUC
National Association of Regulatory Utility Commissioners

Understanding Cybersecurity Preparedness: Questions for Utilities



Lynn P. Costantini
Matthew Acho

June 2019

Acknowledgments

This report was developed under the project “State and Local Innovation and Analysis in Support of Long-Term Energy Planning and Policy,” of the National Association of Regulatory Utility Commissioners (NARUC) Center for Partnerships & Innovation. This material is based on work supported by the U.S. Department of Energy under Award Number DE-OE0000818.

Throughout the preparation process, state commissioners and staff provided NARUC with editorial comments and suggestions. However, the views and opinions expressed herein may not necessarily agree with positions of NARUC or those of the U.S. Department of Energy.

Special thanks to:
Kate Marks, Kirsten Verclas, Victor Calderon, and Jeff Hood, U.S. Department of Energy
Dominic Saebeler and Wei Chen Lin, Illinois Commerce Commission
Hon. Jay Scott Emler, Kansas Corporation Commission
Morris Schreim, Maryland Public Service Commission
Dan Searfoorce and David Alexander, Pennsylvania Public Utility Commission
Hon. Ann Rendahl and Jason Ball, Washington Utilities Commission
Jeff Pillon, National Association of State Energy Officials
David Batz and Ivy Lyn, Edison Electric Institute
The Cadmus Group LLC

Please direct questions regarding this report to Lynn P. Costantini, Deputy Director, NARUC Center for Partnerships and Innovation, at lcostantini@naruc.org, or Matthew Acho, Program Officer at macho@naruc.org.

Disclaimer: 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.

Table of Contents

Preface

NARUC has developed a comprehensive suite of resources, collectively referred to as the Cybersecurity Manual, to help public utility commissions (PUCs or "commissions") gather and evaluate information from utilities about their cybersecurity risk management practices. These evaluations facilitate well-informed PUC decisions regarding the effectiveness of utilities' cyber security preparedness efforts and the prudence of related expenditures.

The Cybersecurity Manual is comprised of five complementary resources. The *Understanding Cybersecurity Preparedness: Questions for Utilities* is one of them. A brief description of each resource follows.

1. ***Cybersecurity Strategy Development Guide* | 2018**
   The Strategy Development Guide defines a roadmap that PUCs can follow to design and implement a structured approach for long-term engagement with utilities on cybersecurity matters. The Guide includes examples from PUCs that demonstrate the process steps and highlights practices that drive successful outcomes.

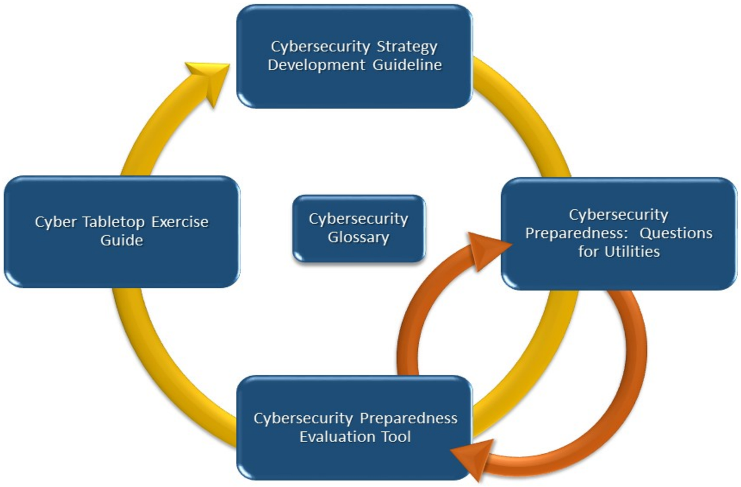
2. ***Understanding Cybersecurity Preparedness: Questions for Utilities* | 2019**
   The Questions for Utilities provides a set of comprehensive, context-sensitive questions that PUCs can ask of a utility to gain a detailed understanding of its current cybersecurity risk management program and practices. The questions build upon and add to those included in prior NARUC publications.

3. ***Cybersecurity Preparedness Evaluation Tool (CPET)* | 2019**
   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.

4. ***Cybersecurity Tabletop Exercise (TTX) Guide* | 2019**
   This guide details the steps that PUCs can take to design and execute an exercise to examine utilities' and other stakeholders' readiness to respond to and recover from a cybersecurity incident. It includes exercise scenarios and examples.

5. ***Cybersecurity Glossary* | 2019**
   The *Glossary* contains cybersecurity terms used throughout the Cybersecurity Manual, as well as "terms of art" that utilities may use during discussions with PUCs.

Figure 1: NARUC Cybersecurity Manual Components


Cybersecurity Strategy Development Guideline
Cybersecurity Preparedness: Questions for Utilities
Cybersecurity Glossary
Cyber Tabletop Exercise Guide
Cybersecurity Preparedness Evaluation Tool

Resources within the Cybersecurity Manual can be used individually but are designed to work together. NARUC's intent is to provide a comprehensive set of assessment tools that, when applied, provide a consistent, complete view of utilities' cybersecurity preparedness. **Figure 1** depicts the complementary, process-oriented relationship among these components.

The content of each component in the Cybersecurity Manual is customizable to meet specific goals, objectives, and requirements that PUCs have established around cybersecurity, complementing resources developed by and for utilities and other practitioners. Geared toward non-technical, policy-oriented users, each component captures information in sufficient detail to support PUC decision making.

Introduction

Public utility commissions are responsible for ensuring adequate, safe and reliable utility services at reasonable rates. As such, they need to know that utilities have effective cybersecurity risk management programs in place to mitigate cybersecurity vulnerabilities, counter malicious cyber threats, and rapidly respond and recover from successful attacks.

From this perspective, it is necessary for utilities to provide their commissions with information that describes their current cyber risk mitigation policies and practices. Commissions should ask probing questions of utilities to identify the extent of utilities' capabilities to address emerging and rapidly evolving threats and vulnerabilities. Together, this knowledge helps commissions identify cybersecurity gaps, spur utilities' adoption of additional mitigation strategies, and encourage improvements over time.

Purpose

Understanding Cybersecurity Preparedness: Questions for Utilities facilitates commissions' discussions with utilities about their cyber risk management programs and implementations. The content builds upon and extends NARUC's *Cybersecurity Primer*, released in 2012 and updated in 2017.[1] The *Primer* sought to explain, without using technical jargon, cybersecurity basics that commissions could build upon to engage utilities in topical discussions. Since the release of the *Primer*, commissions have gained cybersecurity experience and knowledge. Now many are interested in going beyond the basics and exploring utilities' cybersecurity risk management practices in more depth. This document helps commissions take that next step.

The *Questions for Utilities* tool is one component of NARUC's Cyber Manual, a toolkit aimed at helping commissions gather and evaluate information from utilities to inform their decision making about cybersecurity risk management practices and cost effectiveness of cyber security expenditures. The *Questions for Utilities* complements other tools developed as part of the Cyber Manual, especially the *Cybersecurity Preparedness Evaluation Tool* (CPET), which helps commissions assess the maturity of a utility's cybersecurity program, gauge improvements to that program year over year, and evaluate utility decisions and their approaches to planning for and making security-focused investment.

Overview

This document is divided into three parts. Part I identifies key issues that commissions should consider before discussing cybersecurity matters with utilities. Part II presents a set of context-sensitive questions commissions may use as discussion prompts during those discussions. Part III describes post-discussion activities for commission consideration.

The questions in Part II are organized by cyber risk management functions, as shown in **Figure 2**. This organization intentionally aligns with the NIST Cybersecurity Framework,[2] an industry agnostic model rooted in well-established information security principles. The Cybersecurity Framework maps readily to the electric-sector-specific NERC CIP standards[3] and to other popular frameworks such as ISO 27001.[4] It is also compatible with cybersecurity guidance produced by the Department of Energy, such as the Cybersecurity Capability Maturity Model (C2M2).[5]

[1] Cybersecurity: A Primer for State Utility Regulators, Version 3.0, January 2017 (https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F).

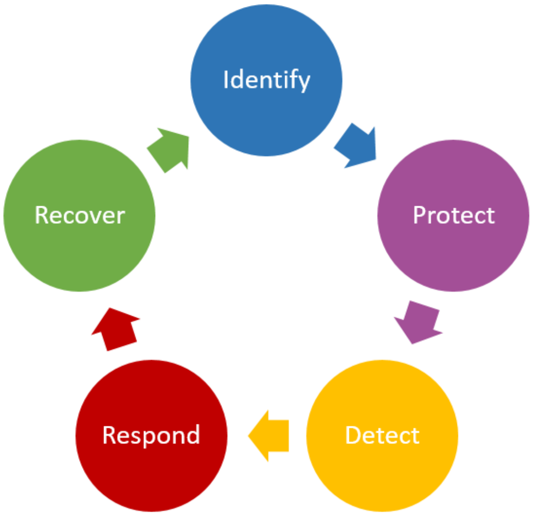
[2] NIST Cybersecurity Framework Version 1.1, April 16, 2018, (https://doi.org/10.6028/NIST.CSWP.04162018).

[3] Reliability Standards for the Bulk Electric Systems of North America, Updated January 9, 2019, https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf.

[4] International Organization for Standardization, https://www.iso.org/isoiec-27001-information-security.html.

[5] https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0.

Figure 2: Cybersecurity Risk Management Cycle



The questions are divided into two categories per risk management process step: 1) policy and plans and 2) implementation and operations. Questions in the policy and plans category address the contents of utilities' documented cybersecurity policies, plans, processes, and procedures. Answers to these questions help commissions understand the strategies, goals, objectives, policies and programmatic plans that a utility has defined to identify and mitigate cyber risks, as well as the criteria they used to decide them. Questions in the second category—implementation and operations—aim to provide insight into operational processes, procedures, and technologies that utilities have in put in place to meet their defined cybersecurity risk management goals and objectives. Asking questions in each of these categories may be useful to identify gaps between utilities' cybersecurity planning and implementation practices. These questions are relevant to both information technology (IT) and operations technology (OT) assets and the environments in which they operate.

Part I. Pre-Engagement Considerations

Before engaging utilities in discussions about cybersecurity, commissions should set clear goals and objectives for the engagement and should define measures of success.[6] Doing so ensures clarity of purpose for both the commission and the utility, and helps both parties effectively prepare beforehand. As part of the pre-engagement planning phase, commissions also should determine where and when these cybersecurity discussions will take place, taking into consideration regulations and rules for meeting with utilities. Other considerations for commissions at this stage include deciding who will participate in the discussions on the commission's behalf and how confidentiality of information will be addressed. Because of the sensitivity of cybersecurity related information, addressing these considerations in advance is of particular importance to utilities. More detail on each of these key topics follow.

Staffing

An important question in the pre-engagement stage is who will represent the commission in its discussions with utilities. Ultimately, these representatives will lead the discussion, pose questions, and review the documentation that utilities provide to support their responses. Selection will depend on the cybersecurity knowledge and technical skills resident within the commission. Commissions may find it useful to form a cross-functional team. In addition to staff with direct cybersecurity responsibilities, including personnel from other units within the commission—utility operations, legal, and IT for example—provides synergy. On the other hand, commissions may opt to hire qualified cybersecurity consultants to lead the engagement, with or without commission personnel in attendance.

Utilities will want the names of commission team members in advance. Knowing this information prior to the engagement will help the utility bring the appropriate level of management and technical skills to the table.

[6] See NARUC's *Cybersecurity Strategy Development Guide*, October 2018, https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204.

Location

Due to the sensitivity of cybersecurity-related information, the setting in which commissions and utilities meet is another important consideration. Utilities may prefer face-to-face meetings over the electronic exchange of potentially sensitive or confidential documents, such as their cybersecurity plans, processes and related diagrams. Location options include commission offices, utility premises, or neutral third-party locations such as state fusion centers, local FBI field offices, or similar secure locations. Factors to weigh include the rules governing such meetings, the utility's preference, and the availability of pre-arranged, off-site locations.

To maximize the time spent together, it may be beneficial to hold the meeting on utility premises. Doing so allows the utility to call upon additional experts should the need arise as the discussion progresses. It also allows the utility to gather and provide additional documentation should it be necessary.

Confidentiality

Before meeting with utilities, commissions should clarify how the discussion will be recorded and who will have access to that information post meeting. Utilities prefer that information pertaining to their cybersecurity plans, practices, and protection technologies remain confidential. Appropriately, utilities are concerned that sensitive security specific information, if publicly released, could allow adversaries to identify, target, and attack potential weaknesses.

To facilitate the unfettered sharing of information, some states have passed legislation that protects cybersecurity data from public disclosure. Others have made administrative rulings for this purpose.[7] In the absence of such protections, commissions may opt to hold cybersecurity related meetings in "listen-only" mode. This means that notes will not be taken during the meeting and the utility retains all documentation. If a commission intends to take notes or remove documentation, it should detail for the utility in advance how it will protect that information from unauthorized access.

Ultimately, the meeting format will depend on a combination of the commission's stated goals, utility preferences, confidentiality protections, and rules and regulations in place for such meetings.

[7] http://www.ncsl.org/research/energy/open-government-laws-and-critical-energy-infrastructure.aspx.

Part II: Questions for Utilities

Cybersecurity risk management is the ongoing process of identifying, assessing, and responding to risk. The goal is to minimize the likelihood of a cyber incident as well as the negative effects should one occur. No single approach or set of technologies exists for this purpose. Utilities must devote resources to develop and implement cybersecurity risk management programs that demonstrate their security priorities and their investment and operational decisions.

For commissions, understanding utilities' cybersecurity risk management practices is helpful to their own decision-making pertaining to utilities' provision of safe, reliable, cost-effective service. The questions contained in this section help commissions probe these issues to provide a better understanding of utilities' overall cyber security preparedness.

For the purposes of this document, questions to ask utilities are organized into five categories that reflect the risk management process steps—called functions—defined in the NIST Cybersecurity Framework.[8] NIST created this framework expressly to improve cybersecurity risk management as it relates to critical infrastructure. It provides a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk.

1. Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
2. Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.
3. Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4. Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
5. Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Although these process steps provide a useful structure to follow, the questions themselves are tailored for commission use. They do not delve into significant detail about unique cybersecurity systems, specific technologies, or customized applications that utilities may employ. Rather, the questions focus on the efficacy of a utility's cybersecurity program.

How to Use the Questions

The questions presented in this document help to spur discussions regarding utilities' cybersecurity preparedness. Commissions may want to tailor the questions to suit the goals and objectives they have set for each engagement with a utility. For example, some commissions may choose to limit questions to one risk management function, whereas others may choose to ask a few questions from each. For first-time engagements, a commission may choose to ask more questions than it would during subsequent meetings.

[8] NIST Cybersecurity Framework Version 1.1, April 16, 2018, (https://doi.org/10.6028/NIST.CSWP.04162018).

Questions by Cybersecurity Risk Management Function

IDENTIFY

Policy and Plans

1. Do you have a cyber risk management program?
- **a.** If so, who leads the program?
- **b.** Is executive leadership actively engaged?
- **c.** Are cybersecurity roles and responsibilities defined?
- **d.** Have you formed a cross-functional team that spans relevant business units to assess risks to and criticality of business functions?
- **e.** Is the program based on a cybersecurity framework (e.g., NIST, NERC CIP)?
- **f.** Is the program integrated into overarching enterprise risk management?
- **g.** Are criteria for defining and managing cybersecurity risk included? If yes, please explain.

2. Have you written and implemented a cybersecurity policy, strategy, or similar governance document?
- If no, are there other organizational policies or similar documents that address cybersecurity, and if so, please describe them.
- If yes, please respond to the following:

a. Describe the contents.
b. Describe the development and approval process.
c. Is the cybersecurity policy, strategy or governance documents reviewed or audited regularly? If yes, please respond to the following questions.
  i. Who performs the review or audit?
  ii. What qualifications are considered when selecting review or audit team members?
  iii. What is the review and audit frequency?
  iv. Who within the company receives the review/audit results?
d. Does your cybersecurity policy or plan address both cyber and physical assets? Does your physical security plan identify critical cyber assets?
e. Do policies, plans, etc., include IT and OT systems?
f. Does your cybersecurity policy or plan require identification of critical facilities and/or cyber assets that are dependent upon IT or automated processing?
g. Does your company have an information classification and handling policy?
f. Do you document cybersecurity criteria for vendor and device selection? If yes, describe the criteria.

3. Does your company include in its procurement contract language cybersecurity requirements for IT and OT assets?
- **a.** Do you have specific guidance that you follow to ensure that your procurement language is both specific and comprehensive enough to result in acquiring secure components and systems?

4. Do you leverage resources such as DOE's C2M2 or Risk Management Process for Cybersecurity?

Implementation and Operations

1. Have resources (funding, personnel, technology) been dedicated to meet cybersecurity risk management objectives?
- **a.** Are personnel dedicated full time, part-time, or as part of other duties?
- **b.** Is funding commensurate with cybersecurity risk management objectives? Are funding levels consistent?

2. Does an asset inventory exist?
- **a** If so, how frequently is the inventory reviewed and updated?
- **b.** Have asset criticality levels been assigned? If so, how have the criticality levels been determined?

3. Has your organization conducted a risk assessment of its information systems, control systems, and other networked systems?
- **a.** Please describe the process.
- **b.** Have you worked with, or used resources provided by, a federal agency (e.g., ICS-CERT/CSET, DHS C3 Program, FERC Architectural Reviews) to conduct a cybersecurity assessment?
- **c.** Do you maintain a register of identified cyber risks?
  - **i.** Do you review and update the risk register on a regular basis?
  - **ii.** What is the review cycle?

4. Do you evaluate cyber risks during the installation of new systems, during system upgrades and replacement, and during end-of-life decommissioning?

5. Does your assessment identify IT/OT supplier and customer dependencies and associated risk?
- **a.** How do you conduct your risk assessment of these organizations and what constitutes a "red-flag" for working with them?

6. Are there third-party providers of services whose cybersecurity controls are beyond your utility's ability to monitor or ensure?
- **a.** How do you verify that these companies have adequate cyber controls?
- **b.** Who handles that assessment?

7. Do you require end-user training on cybersecurity for all employees, either as part of general training or specifically on the topic of computer security and company policy?
- **a** Who conducts your training?
- **b.** What is the content of these trainings?
- **c.** Does this training involve lessons learned from actual incidents?
- **d.** When/how often do you conduct training?
- **e.** Do you provide resources to improve end-user awareness of phishing, malware, indicators of compromise, and procedures in the event of a potential breach? If so, would you provide a description of these resources?

8. Do you require specialized cybersecurity training for personnel with IT or OT responsibilities?
- **a.** Who conducts specialized training?
- **b.** What is the content of specialized training?
- **c.** When/how often do you conduct specialized training?

PROTECT

Policy and Plans

1. **Do you budget for cybersecurity tools and technology separately from IT?**
   a. If so, who is responsible for cybersecurity budgeting?
   b. What does the cybersecurity budgeting process look like?
   c. Are expenditures for cybersecurity identified in PUC rate recovery requests?
2. **Are you subject to NERC CIP-002 through CIP-014?**
   a. Have you been the subject of a NERC CIP audit? If so, are you willing to share the results of that audit?
   b. Are you using elements of NERC CIP as a guideline for protecting electric distribution systems assets? If so how?
   c. Do other mandatory cybersecurity requirements apply? If so, please describe them.
3. **Have you implemented a change management process?**
   a. Describe the process.
   b. Are change requests reviewed by a cross-functional team?
   c. Who approves change requests?
4. **Do you have a documented records retention policy?**
5. **Do you have a vulnerability management plan?**
   a. Does the plan include requirements for patch management?
      i. Does the patch management plan include criteria for prioritizing the review and implementation of patches? If so, explain the criteria.

Implementation and Operations

1. **Have you implemented tools, technologies, processes, and procedures (i.e., controls) to meet cybersecurity policy requirements aimed at protecting critical functions or assets? If yes, please respond to the following:**
   a. Has defense-in-depth been implemented? If so, describe your network segmentation model that protects critical assets and the functions they support.
      i. If applicable, define the segmentation between IT and OT networks.
      ii. How is access to critical IT and OT assets controlled?
      iii. How are logical and physical connections between network segments identified and monitored?
   b. Do you control and monitor privileged accounts?
      i. If yes, please describe how control and monitoring is implemented.
      ii. Are principles of least privilege and need to know incorporated?
      iii. How is third-party access controlled and managed?
   c. Have you documented baseline security configurations for critical cyber assets?
   d. Do you have dedicated tools and resources for managing vulnerabilities?
      i. If so, who conducts the assessments?
      ii. How are identified vulnerabilities addressed?
      iii. Are patches implemented according to prescribed requirements?
   e. Are data backed up (SAN, NAS, Cloud)? If yes, how frequently is restoration from backups tested?
2. **Is cybersecurity addressed differently for IT and OT systems? If so, describe the differences and the advantages that different treatment provides.**
3. **Do you assign priority to certain systems when implementing new cybersecurity measures**?
   a. How are those priorities determined?
   b. Are priorities reviewed periodically?
4. **Is cybersecurity maintained during the replacement and upgrade of assets, systems, and networks?**
   a. How are these processes implemented?
   b. Who usually handles these upgrades?
   c. If smart meters are in place, how are upgrades performed and verified?
5. **Are personnel surety/background checking performed for those with access to critical assets?**
   a. What screening criteria are used?
   b. Are vendors and other third parties who have access to key cyber systems screened? If yes, who performs the screening? What criteria are used?
6. **Do you collect personally identifiable information (PII) electronically?**
   a. If yes, how long is PII retained?
   b. What are the processes and procedures in place for deleting PII?

DETECT

Policy and Plans

1. **Have you developed policies and procedures regarding cybersecurity event detection activities, including roles and responsibilities, oversight, and communications, to rapidly detect and mitigate cybersecurity incidents? If so, please describe**
   - **a.** the classification scheme for identifying and reporting cyber events, including thresholds;
   - **b.** the system and network monitoring requirements; and
   - **c.** the frequency of reviews and updates to policies and procedures.
2. **Are you currently required to report any cyber incidents to any federal or state agencies?**
   - **a.** Do you notify law enforcement?
   - **b.** Do you notify the PUC?
   - **c.** Do you notify other utilities in your region?
   - **d.** Do you notify US-CERT?
   - **e.** What are the reporting thresholds?
   - **f.** Have you defined the details that will be included in incident reports? If so, what are they? Do you tailor them for each report recipient?

Implementation and Operations

1. **Have you implemented processes and procedures for identifying and tracking suspicious cyber activity?**
   - **a.** Have you deployed a SIEM (Security Incident and Event Management) or similar automated log analytic tools for log aggregation and consolidation from multiple assets for correlation and analysis?
   - **b.** Are local- and host-based intrusion detection and protection systems in place?
   - **c.** Are suspicious activity thresholds assessed and updated in accordance with policies?
2. **Do you conduct regular external and internal penetration tests to identify weakness that can be exploited?**
   - **a** Who conducts these tests?
   - **b.** How are findings prioritized and corrected?
3. **Do you coordinate with other organizations to augment threat detection activities?**
   - **a.** If yes, identify these organizations and describe sharing mechanisms.
   - **b.** Do you belong to one or more sector-specific information sharing and analysis centers (ISAC)? If so, which ones?
     - **i.** Who reviews threat alerts and warnings?
     - **ii.** How are threat alerts and warnings addressed?

RESPOND

Policy and Plans

1. **Do you have cyber incident response policies and plans in place for minimizing the effects of a cyber incident?**
   - **a.** If yes, are roles and responsibilities for recovery defined?
   - **b.** Are incident severity thresholds defined?
   - **c.** Are escalation criteria defined?
   - **d.** Are mandatory third-party incident notification requirements documented (e.g., to PUC, SEC)?
   - **e.** Does your response plan include interactions with third-party service providers?
2. **Do your response plans include the use of alternative methods for meeting critical functions in the absence of IT or communication technology?**
   - **a.** If yes, describe these alternative methods and how you plan to leverage them during a cyber emergency.
3. **Do you have lists of identified points of contact for cybersecurity?**
   - **a.** How do you maintain contact lists?
   - **b.** Do the lists include external contacts (e.g., law enforcement, U.S. CERT, etc.)?
   - **c.** Do you belong to a cyber mutual assistance group? If so, please explain the participation requirements. Are non-disclosure agreements (NDA) mandatory?

Implementation and Operations

1. **Is your cyber incident response plan tested regularly?**
   - **a.** When was the last time the plan was tested?
   - **b.** How did you test the plan (e.g., plan walk-through, table top exercise, functional exercise)?
   - **c.** Were third-party service providers involved?
   - **d**. How did you address lessons learned?
2. **Is training provided to personnel who are assigned response duties?**
   - **a.** If yes, do these individuals go through more extensive cybersecurity training than those without response duties? If so, describe the scope of specialized training.
   - **b.** Does your company rely on third parties to perform response activities involving IT or OT assets?
3. **Is cybersecurity assured during a response effort? If so, how?**
4. **Have you experienced a reportable cyber incident?**
   - **a.** Describe the incident. Were OT assets involved?
   - **b.** How quickly were incident notifications made; how were they made, and who was notified? Did these notifications follow documented incident declaration and response procedures?
   - **c.** Were mandatory incident notifications made to external parties as required?
   - **d.** Were incident response actions coordinated with third-party vendors, industry partners, or other external parties? Is so, please describe.

RECOVER

Policy and Plans

1. **Have you identified minimal operational functionality for recovery of critical assets?**
2. **Have recovery activities been consolidated into formal continuity and recovery plans?**
   - **a.** If so, are those policies and plans aligned with overarching business continuity plans?
   - **b.** Are restoration priorities and recovery objectives defined?
   - **c.** Are roles and responsibilities defined?
   - **d.** Are legal and regulatory staff included?
   - **e.** Are third-party vendors included in recovery planning activities?
3. **Do you have alternative locations ready should it be necessary to relocate operational control to ensure service delivery?**
   - **a.** If so, please describe these alternative locations (i.e., Are they cold sites? Hot sites?)
   - **b.** Have you established declaration criteria that defines when to move operations and the authorities for making that declaration?
   - **c.** Are return-to-normal criteria included?
4. **Do you invest in cyber insurance**?
   - **a.** If so, how do you determine the appropriate level of coverage for your organization?

Implementation and Operations

1. **Have you ever implemented recovery plans in response to a cyber incident?**
   - **a.** If so, please describe that recovery event. Were OT assets involved?
   - **b.** Were recovery point objectives met?
   - **c.** Were recovery activities coordinated with third-party vendors, industry partners or other external parties? If so, please describe.
   - **d.** Were forensics performed and if so, who performed them?
   - **e.** Were capability gaps recognized and corrective actions incorporated into recovery plans?
2. **Do you regularly test your cyber incident recovery plan?**
   - **a.** When was the last time the plan was tested?
   - **b.** How did you test the plan (e.g., structured walk-through, tabletop exercise, functional exercise)?
   - **c.** Were third-party service providers involved?
   - **d.** Are recovery actions analyzed, corrective actions recommended, and recovery plans updated?
3. **Is training provided to personnel who are assigned recovery duties?**
   - **a.** If yes, do these individuals go through more extensive cybersecurity training than those without response duties? Describe the scope of specialized training.
   - **b.** Does your company rely on third parties to perform restoration activities involving IT or OT assets?
   - **c.** Do you contract with a third party to perform cyber forensics?
     - **i.** If so, who receives the forensic analysis?
     - **ii.** How are forensic results addressed in protection, response, and recovery plans?
     - **iii.** Do you communicate forensic results to relevant internal and external stakeholders? If so, how?

Part III: Post-Engagement Considerations

Responses to detailed planning and implementation questions provide the necessary input for PUCs to assess a utility's current state of cybersecurity preparedness. They also indicate the utility's capabilities to manage emerging cybersecurity risks effectively over time. NARUC's *Cybersecurity Preparedness Evaluation Tool* (CPET) provides a structured, repeatable mechanism to assess responses to cybersecurity questions and assign qualitative indicators of capabilities—called maturity levels—to core risk management functions. Used together, the *Questions for Utilities* and CPET provide a holistic view of a utility's cybersecurity risk management program.

Using a structured approach lends consistency to a PUC's assessment of a utility's cybersecurity program. It also provides the ability to gauge year-over-year improvements to that program. Comparisons between utilities are unwarranted, however, as each utility's operating environment and cybersecurity program are unique.

Additionally, commissions benefit when discussions with utilities about their cybersecurity programs take place regularly. A good rule of thumb is to meet once per year, but more frequent meetings are acceptable. By working closely with utilities over time, commissions gain a more detailed knowledge of their cybersecurity risk management practices, as well as a richer appreciation of evolving risks and responses. Ideally, PUCs questions will evolve as they grow more familiar with their utilities' cyber capabilities. It is useful, however, for PUCs to revisit subject areas consistently so gaps or improvements are recognized.

Lastly, sustained engagement builds trust and encourages transparency. As such, it may be helpful for commissions to ask utilities for feedback following each engagement. A focus on process improvements and relationship building is likely to enhance the outcomes of future discussions on cybersecurity risk management.

Appendix A.

Acroynms

CIP	Critical Infrastructure Protection
CPET	Cybersecurity Preparedness Evaluation Tool
DOE	U.S. Department of Energy
FERC	Federal Energy Regulatory Commission
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electricity Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operational Technology
PUC	Public Utility Commission
US-CERT	U.S. Computer Emergency Readiness Team

NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

DEDICATED TO PUBLIC SERVICE

1889