NARUC's Cybersecurity Resources: Putting Knowledge into Action

Jody Raines, Sr. Cybersecurity Policy Specialist

April 5, 2023

- ✓ Energy infrastructure is critical to the security of a state and represents a common good.
- ✓ New technology is driving change.
- ✓ Change can be risky.
- ✓ State regulators have a role in managing risks to energy infrastructure.

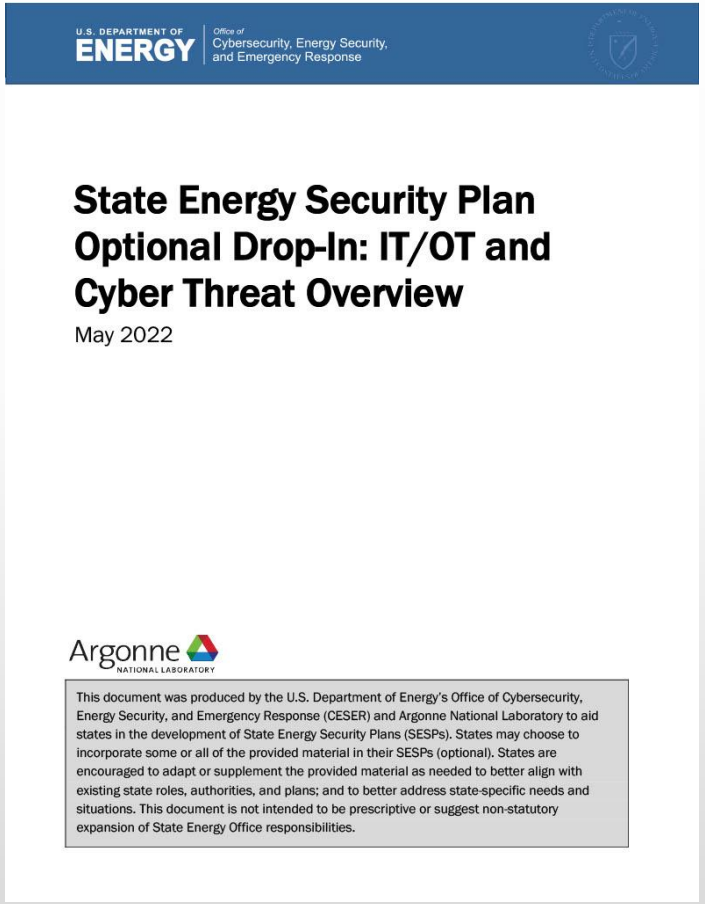
PUC Job Description

PUC: Ensures safe, reliable utility service at fair and reasonable rates.

(NARUC's job is to assist)

How Do I Use This With The ESP?

- Energy Security Plan – Optional Drop-In IT/OT and Cyber Threat Overview
- Need information to fill in the blanks, for example: “describe the mechanisms by which the state receives, analyzes and/or shares information with energy and emergency officials and energy industry partners”


U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

State Energy Security Plan Optional Drop-In: IT/OT and Cyber Threat Overview

May 2022

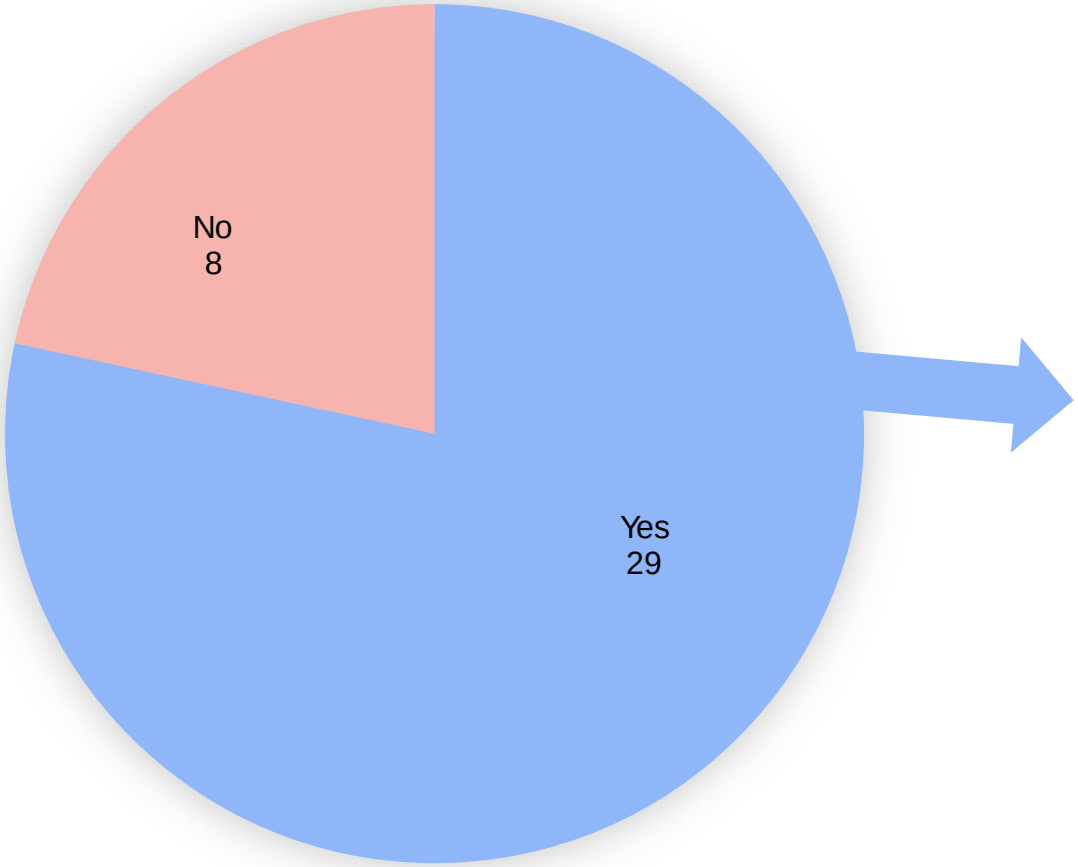
Argonne NATIONAL LABORATORY

This document was produced by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Argonne National Laboratory to aid states in the development of State Energy Security Plans (SESPs). States may choose to incorporate some or all of the provided material in their SESPs (optional). States are encouraged to adapt or supplement the provided material as needed to better align with existing state roles, authorities, and plans; and to better address state-specific needs and situations. This document is not intended to be prescriptive or suggest non-statutory expansion of State Energy Office responsibilities.

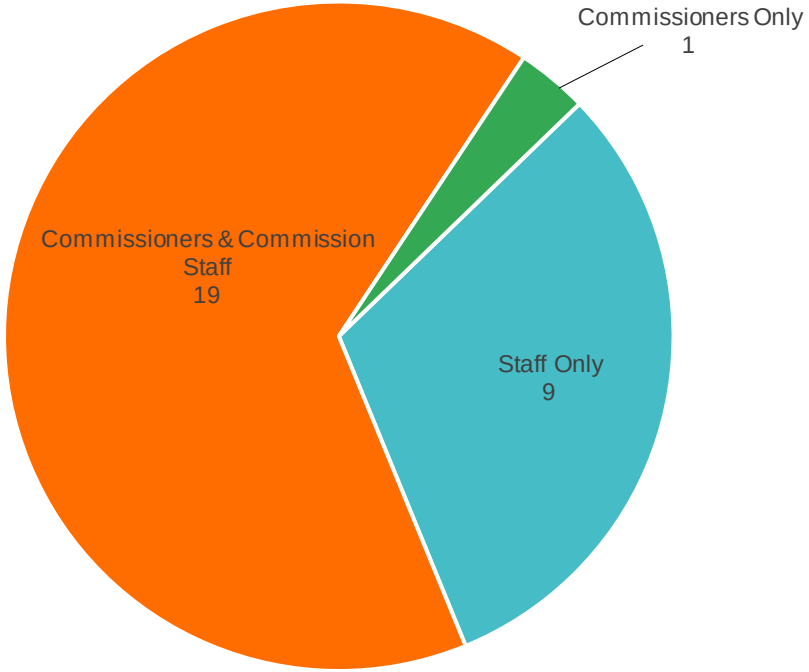
Sharing Information

- Is Your PUC Already Engaged in These Discussions?
- Each state is different.
- Open the dialogue.
- Collaboration and Coordination.

Outside of docketed proceedings, does your commission meet with your regulated utilities to discuss cybersecurity risk management?

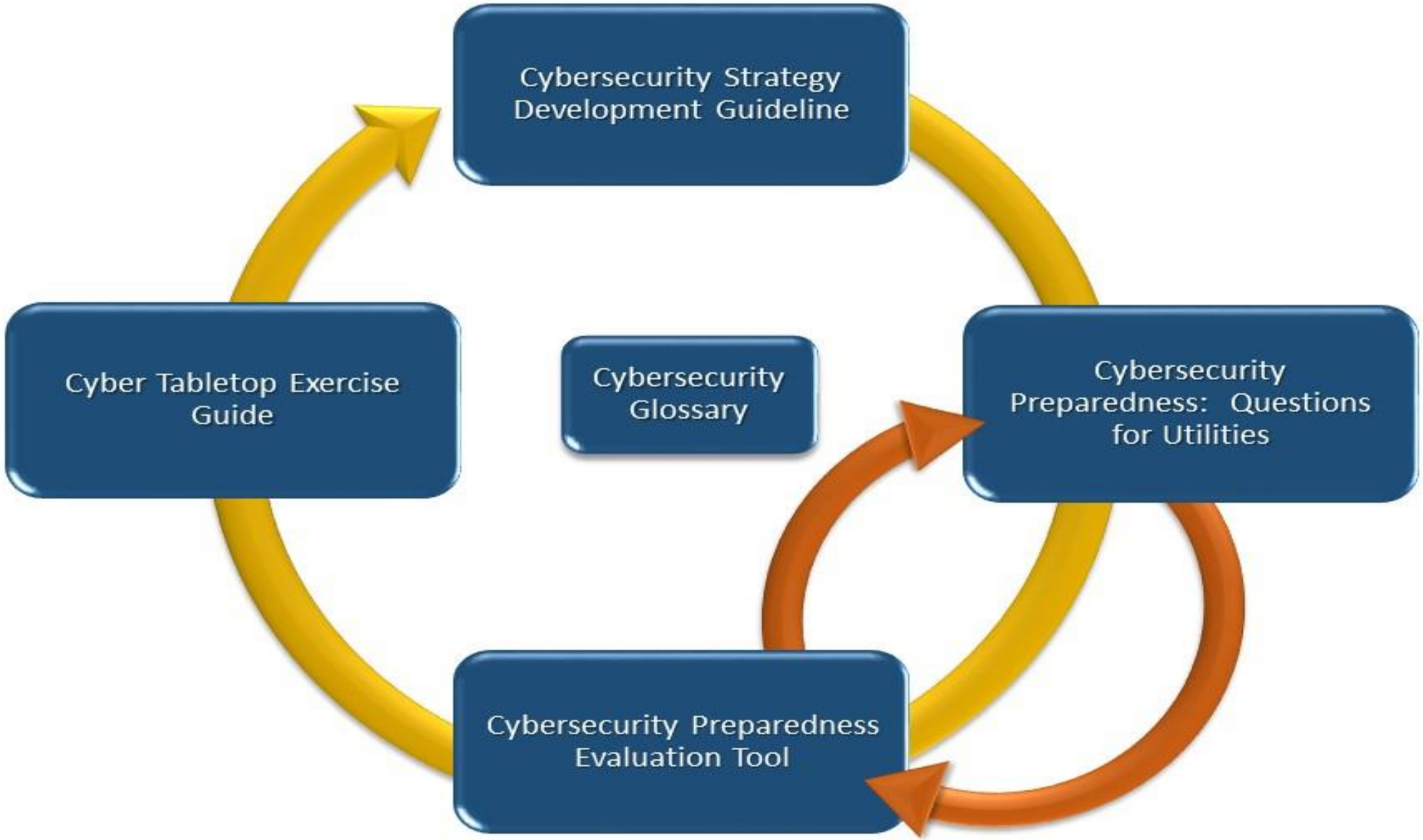


If yes, who is involved?

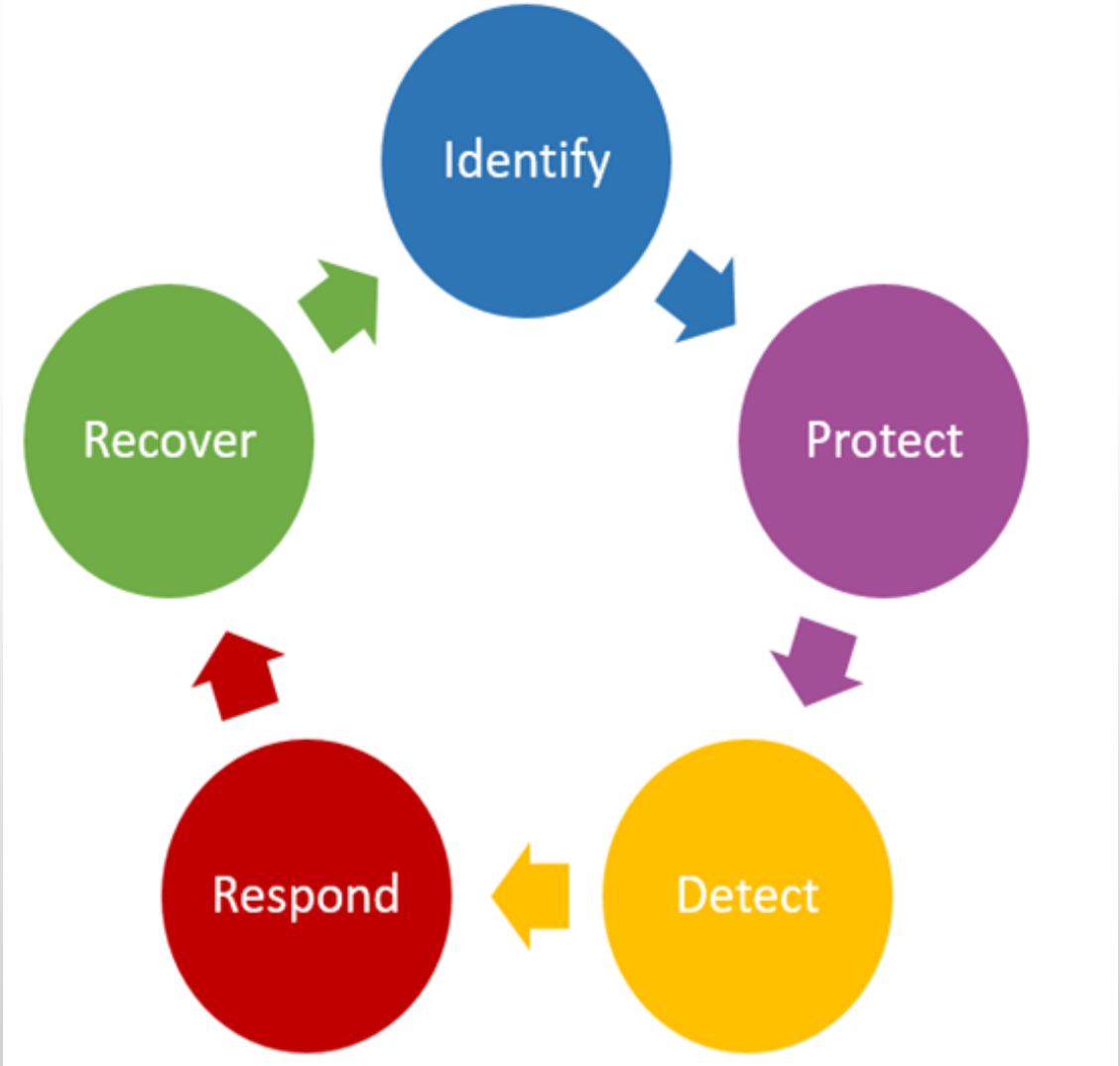


NARUC's Cybersecurity Manual

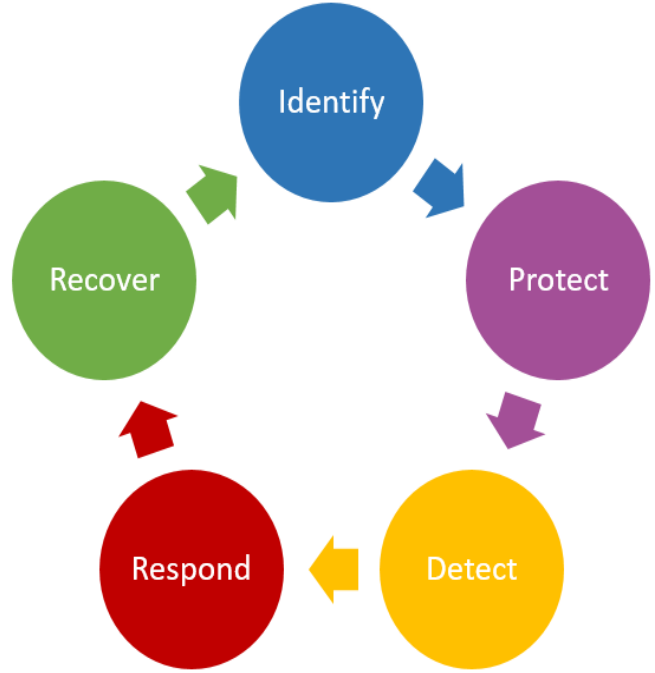
- Turns foundational cybersecurity concepts into useful tools to drive action
- Set of individual tools tailored to public utility commissions
- Tools purposefully fit together to optimize value


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

RISK MANAGEMENT CYCLE

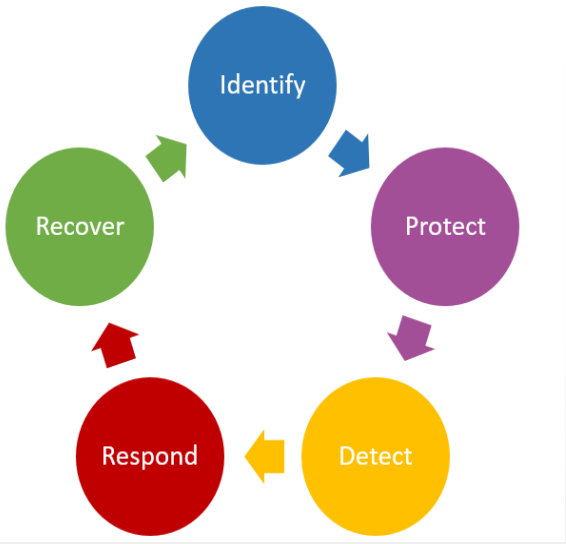


Understanding Cybersecurity Preparedness: Questions for Utilities



Risk Management Cycle

- Provides series of specific, contextual questions to ask utilities about their cyber risk management program.
- Drives a deeper understanding of utilities' overall cybersecurity preparedness.
- Aids PUC decision-making about cybersecurity investments.
- Feeds into Cybersecurity Preparedness Evaluation Tool (CPET).



IDENTIFY

IDENTIFY

Policy and Plans

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?

Implementation and Operations

Have resources (funding, personnel, technology) been dedicated to meet cybersecurity risk management objectives?

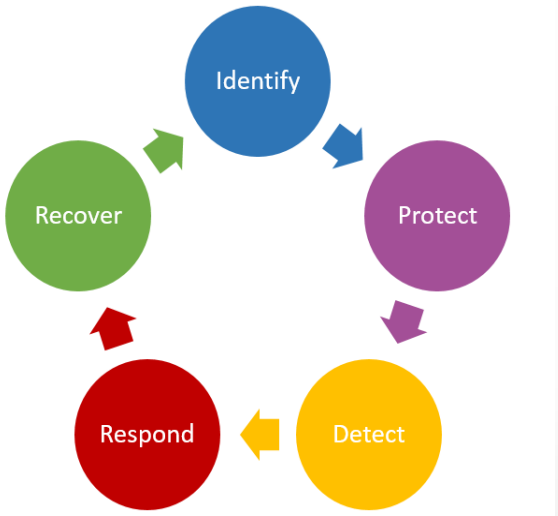
a. Are personnel dedicated full time, part-time, or as part of other duties?

b. Is funding commensurate with cybersecurity risk management objectives? Are funding levels consistent?

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?



RESPOND

Respond

Policy and Plans

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?

Implementation and Operations

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?

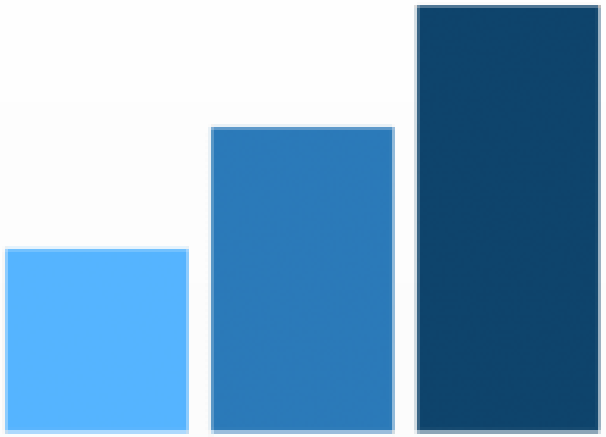
d. How did you address lessons learned?

Is training provided to personnel who are assigned response duties?

If yes, do these individuals go through more extensive cybersecurity training than those without response duties? If so, describe the scope of specialized training.

Cybersecurity Preparedness Evaluation Tool (CPET)

- Provides indicators of a utility's cybersecurity program maturity
  - for non-technical audiences
  - based on C2M2
- Supports PUCs understanding of utilities' current level of cybersecurity preparedness
- Provides means of evaluating performance improvements year over year.
- Uses input from **Questions for Utilities**.



C2M2

Cybersecurity Capability Maturity Model

What is C2M2?

- The Cybersecurity Capability Maturity Model (C2M2) is a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments.

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Developed by the Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Maturity Levels

Maturity Rating	Definition
No Criteria	The utility does not have any policies or plans related to this topic or does not conduct any technical activities related to this topic.
No Information	The utility has not shared sufficient information and, as such, the commission is unable to assign a maturity level.
Level 1: Initial	The utility's practices are informal, uncoordinated, and/or ad hoc and display limited awareness with little or no internal or external coordination.
Level 2: Established	The utility's practices meet minimum resource requirements, are organized to address a strategic need or specific guidance, and may align to an established strategy approved by management with informal information sharing and coordination.
Level 3: Mature	The utility's practices are formally defined, organized, and regularly updated across the organization; prioritized according to needs; adequately resourced, incorporate industry best practices, and are championed by leadership.
Level 4: Optimized	The utility's practices are proactive, informed by objective feedback, embody a culture of continuous improvement, reviewed, and adapted regularly based on lessons learned, and can serve as industry best practices.

Core Function: Identify

Topic Area:	Policy and Plans	Implementation and Operations
Governance	Level 1: Initial	Level 2: Established
Supply Chain and Procurement	Level 2: Established	Level 3: Mature
Risk Management	Level 4: Optimized	Level 4: Optimized
Voluntary/Legal Compliance	No Information	No Criteria
Monitoring and Detection	Level 4: Optimized	Level 3: Mature
…	…	…

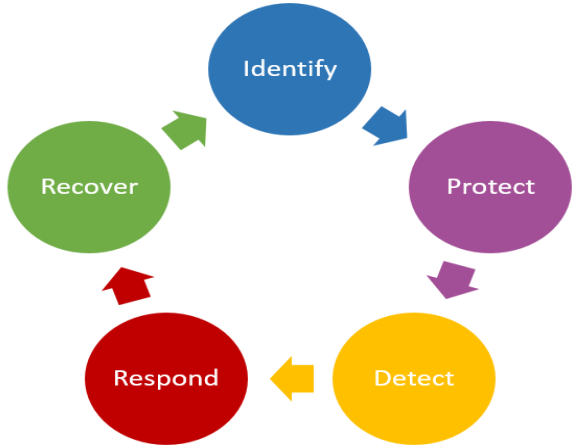
Mock Session

Cybersecurity Questions for Utilities & Cybersecurity Preparedness Evaluation Tool (CPET) Exercise

Overview of Exercise

NARUC's "Actors Guild" will act out a mock interaction between a PUC and a jurisdictional utility -- Forrest State Utility Commission and Pinecone Power.

They'll ask questions within the
Identify, Respond and **Recover** Function
-- Governance,
-- Cyber Incident Response
-- Incident Recovery



YOUR CHALLENGE: Listen carefully to the answers to develop a CPET maturity in each of these areas, based on the answers you hear from Pinecone Power.
Together, we'll review scoring.

Review – CPET Maturity Levels

Maturity Rating	Definition
No Criteria	The utility **does not have any** policies or plans related to this topic or does not conduct any technical activities related to this topic.
No Information	The utility has not shared sufficient information and, as such, the commission is unable to assign a maturity level.
Level 1: Initial	The utility's practices are **informal, uncoordinated, and/or ad hoc** and display limited awareness with little or no internal or external coordination.
Level 2: Established	The utility's practices **meet minimum resource requirements**, are **organized** to address a strategic need or specific guidance, and may align to an e**stablished strategy** approved by management with informal information sharing and coordination.
Level 3: Mature	The utility's practices are **formally defined, organized, and regularly updated** across the organization; prioritized according to needs; adequately resourced, incorporate industry best practices, and are championed by leadership.
Level 4: Optimized	The utility's practices are proactive, informed by objective feedback, embody a culture of **continuous improvement**, reviewed, and adapted regularly based on lessons learned, and can serve as industry best practices.

Actors Guild

Forrest State Utility Commission

- Cybersecurity Program Manager
- Commission’s Chief Engineer

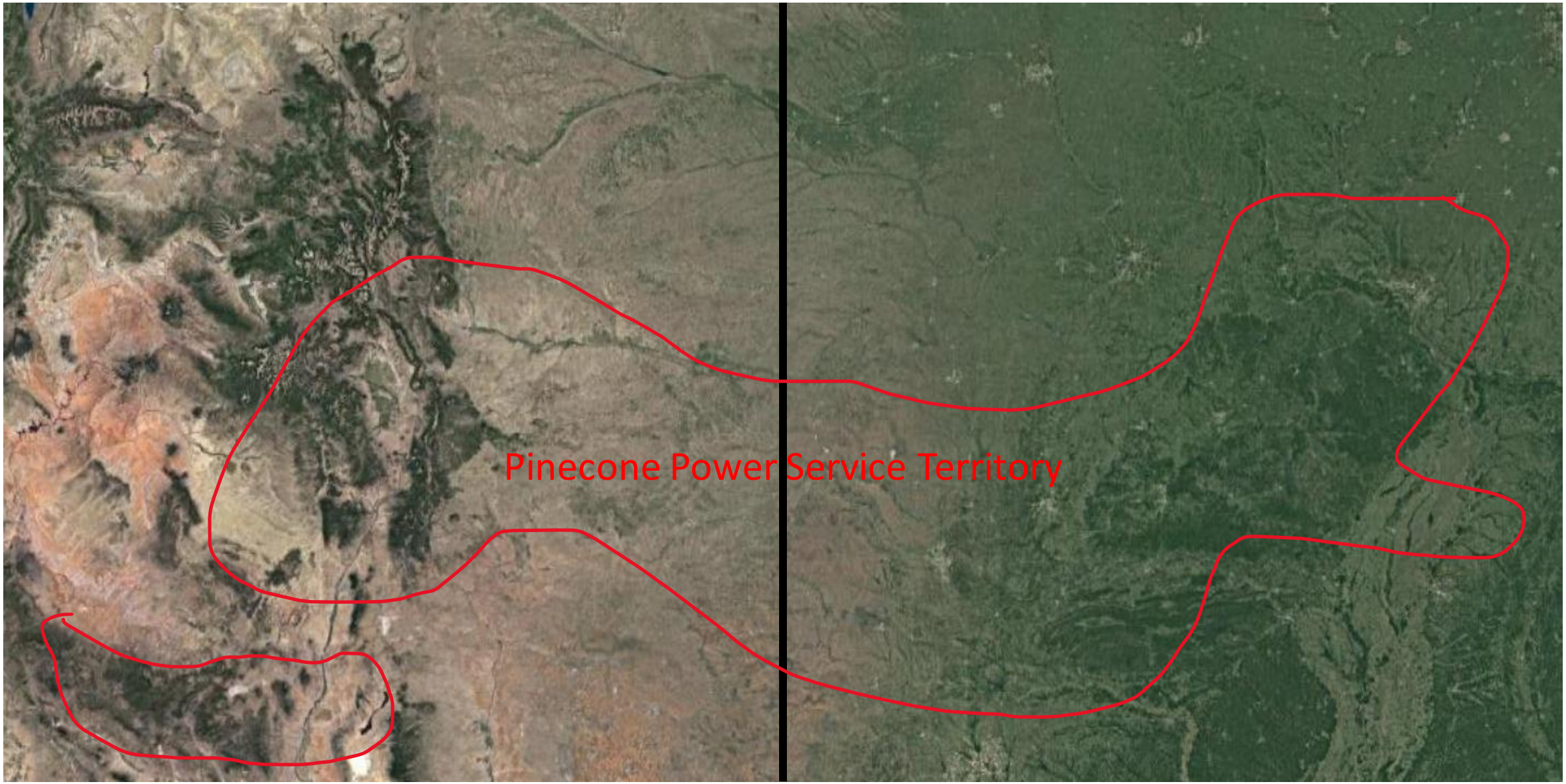
Pinecone Power

– Director of Cybersecurity
– Cybersecurity Engineer
– Chief Legal Counsel

MOCK SESSION LIVE

Mountain State

Forrest State



MOCK SESSION LIVE

Evaluation Criteria: Governance		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Has plans and policies within its IT or security department that assign responsibilities for cybersecurity. ❑ Has dedicated security policies that govern IT and OT systems.	**LEVEL 1: Initial**	❑ Staffed with part-time or multi-duty individuals to manage cybersecurity and does not have a dedicated budget.
❑ Has a cybersecurity plan or strategy that includes an organizational structure stretching beyond IT and/or security departments that outlines the roles and responsibilities related to cybersecurity and information protection.	**LEVEL 2: Established**	❑ Minimally staffed or resourced with budgeted full-time cybersecurity professionals and associated expenses.
❑ Regularly reviews, updates, and improves its cybersecurity plan, strategy, and other governance. ❑ Identifies relevant external stakeholders for cybersecurity events and effectively coordinates cybersecurity roles and responsibilities with external partners.	**LEVEL 3: Mature**	❑ Fully staffed or resourced with budgeted full-time employees who understand the technical, legal, and regulatory requirements regarding cybersecurity.
❑ Identifies a clear policy for incorporating senior leadership during a cybersecurity incident, meeting pre-identified thresholds, and has clearly outlined their roles and responsibilities with respect to providing strategic support for incident response activities.	**LEVEL 4: Optimized**	❑ Senior leadership is actively engaged with cybersecurity activities by championing budgets, taking ownership of plans and policies, and/or regularly meeting to discuss the utility's cybersecurity posture.

TIME OUT

Evaluation Criteria: Governance		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
✓ Has plans and policies within its IT or security department that assign responsibilities for cybersecurity. ✓ Has dedicated security policies that govern IT and OT systems.	**LEVEL 1: Initial**	✓ Staffed with part-time or multi-duty individuals to manage cybersecurity and does not have a dedicated budget.
✓ Has a cybersecurity plan or strategy that includes an organizational structure stretching beyond IT and/or security departments that outlines the roles and responsibilities related to cybersecurity and information protection.	**LEVEL 2: Established**	✓ Minimally staffed or resourced with budgeted full-time cybersecurity professionals and associated expenses.
✓ Regularly reviews, updates, and improves its cybersecurity plan, strategy, and other governance. ✓ Identifies relevant external stakeholders for cybersecurity events and effectively coordinates cybersecurity roles and responsibilities with external partners.	**LEVEL 3: Mature**	✓ Fully staffed or resourced with budgeted full-time employees who understand the technical, legal, and regulatory requirements regarding cybersecurity.
❑ Identifies a clear policy for incorporating senior leadership during a cybersecurity incident, meeting pre-identified thresholds, and has clearly outlined their roles and responsibilities with respect to providing strategic support for incident response activities.	**LEVEL 4: Optimized**	❑ Senior leadership is actively engaged with cybersecurity activities by championing budgets, taking ownership of plans and policies, and/or regularly meeting to discuss the utility's cybersecurity posture.

MOCK SESSION LIVE

Evaluation Criteria: Cyber Incident Response		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ The utility does not have policy or plans related to this topic.	**No Criteria**	❑ The utility has no technical activities related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Uses a generic incident response plan that includes some guidance for cyber incidents.	**LEVEL 1: Initial**	❑ Meets baseline reporting requirements of escalated cybersecurity incidents.
❑ Establishes a dedicated cyber incident response plan that identifies roles and responsibilities for specific personnel and includes response procedures for escalation, containment, and eradication of the threat, including requirements of third-party vendors or service providers. ❑ Establishes and formalizes the criteria for incident declaration and escalation.	**LEVEL 2: Established**	❑ Logs, tracks, and reports cybersecurity events and incidents in a manner consistent with the response plans. ❑ Provides training for personnel with specific response duties. ❑ Leverages law enforcement, government, vendor, or external industry resources for incident response.
❑ Requires that cyber incident response plan is updated and exercised intermittently, incorporating lessons learned from previous incidents or exercises.	**LEVEL 3: Mature**	❑ Maintains a dedicated cybersecurity response team that has the knowledge and resources to contain detected incidents and conduct a coordinated response. ❑ Identifies lessons learned after an incident.
❑ Requires that cyber incident response plans are exercised annually. ❑ Establishes procedures and processes for collecting and analyzing information to mitigate future incidents.	**LEVEL 4: Optimized**	❑ Ensures cyber response team coordinates with external agencies to support industry-wide response efforts. ❑ Establishes cyber mutual aid agreements and/or non-disclosure agreements with key stakeholders.

TIME OUT

Evaluation Criteria: Cyber Incident Response		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ The utility does not have policy or plans related to this topic.	**No Criteria**	❑ The utility has no technical activities related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
☑ Uses a generic incident response plan that includes some guidance for cyber incidents.	**LEVEL 1: Initial**	☑ Meets baseline reporting requirements of escalated cybersecurity incidents.
☑ Establishes a dedicated cyber incident response plan that identifies roles and responsibilities for specific personnel and includes response procedures for escalation, containment, and eradication of the threat, including requirements of third-party vendors or service providers. ☑ Establishes and formalizes the criteria for incident declaration and escalation.	**LEVEL 2: Established**	☑ Logs, tracks, and reports cybersecurity events and incidents in a manner consistent with the response plans. ☑ Provides training for personnel with specific response duties. ☑ Leverages law enforcement, government, vendor, or external industry resources for incident response.
☑ Requires that cyber incident response plan is updated and exercised intermittently, incorporating lessons learned from previous incidents or exercises.	**LEVEL 3: Mature**	❑ Maintains a dedicated cybersecurity response team that has the knowledge and resources to contain detected incidents and conduct a coordinated response. ❑ Identifies lessons learned after an incident.
❑ Requires that cyber incident response plans are exercised annually. ❑ Establishes procedures and processes for collecting and analyzing information to mitigate future incidents.	**LEVEL 4: Optimized**	❑ Ensures cyber response team coordinates with external agencies to support industry-wide response efforts. ❑ Establishes cyber mutual aid agreements and/or non-disclosure agreements with key stakeholders.

LAST ONE

MOCK SESSION LIVE

Evaluation Criteria: Incident Recovery		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic
❑ Did not share information.	**No Information**	❑ Did not share information
❑ Has generic recovery and continuity plans that meet basic requirements.	**LEVEL 1: Initial**	❑ Provides training for personnel with recovery process responsibilities
❑ Develops formal plans for continuity and recovery that reflect specific restoration priorities and include reconstitution measures. ❑ Incorporates lessons learned and corrective actions from real events into continuity and recovery plans. ❑ Identifies the activities necessary to sustain the minimal functions of operations during recovery operations and restoration of critical assets.	**LEVEL 2: Established**	❑ Demonstrates the capabilities and possesses resources to complete the minimum activities necessary to return to normal operations. ❑ Tests continuity and recovery plans by drilling/exercising capabilities.
❑ Outlines specific recovery objectives and priorities in recovery and continuity plans, such as recovery time and point objectives, and IT/OT system recovery priorities. ❑ Recovery and continuity plans include alternative locations for operational control to ensure continuous service delivery.	**LEVEL 3: Mature**	❑ Compares results of continuity plan activation to recovery objectives to assess effectiveness. ❑ Conducts after-action reporting to identify and assess capability gaps and areas for improvement.
❑ Identifies likely impacts of cyber events and incorporates considerations into recovery planning. ❑ Conducts an annual review of mission critical functions and updates recovery and continuity plans.	**LEVEL 4: Optimized**	❑ Contracts with third party organizations to perform additional cyber forensics beyond the scope of internal capabilities. ❑ Prioritizes continuous improvement as part of its culture.

TIME OUT

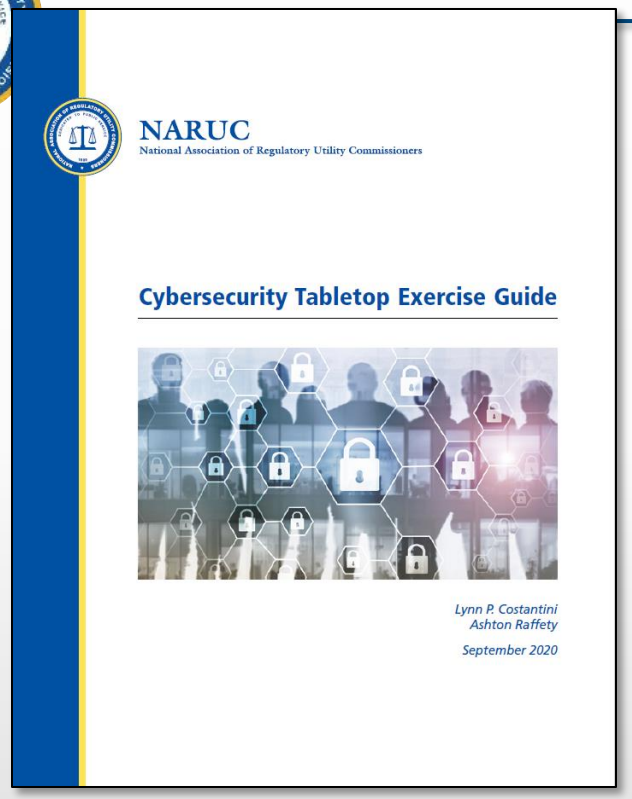
Evaluation Criteria: Incident Recovery		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic
❑ Did not share information.	**No Information**	❑ Did not share information
❑ Has generic recovery and continuity plans that meet basic requirements.	**LEVEL 1: Initial**	❑ Provides training for personnel with recovery process responsibilities
❑ Develops formal plans for continuity and recovery that reflect specific restoration priorities and include reconstitution measures. ❑ Incorporates lessons learned and corrective actions from real events into continuity and recovery plans. ❑ Identifies the activities necessary to sustain the minimal functions of operations during recovery operations and restoration of critical assets.	**LEVEL 2: Established**	❑ Demonstrates the capabilities and possesses resources to complete the minimum activities necessary to return to normal operations. ❑ Tests continuity and recovery plans by drilling/exercising capabilities.
❑ Outlines specific recovery objectives and priorities in recovery and continuity plans, such as recovery time and point objectives, and IT/OT system recovery priorities. ❑ Recovery and continuity plans include alternative locations for operational control to ensure continuous service delivery.	**LEVEL 3: Mature**	❑ Compares results of continuity plan activation to recovery objectives to assess effectiveness. ❑ Conducts after-action reporting to identify and assess capability gaps and areas for improvement.
❑ Identifies likely impacts of cyber events and incorporates considerations into recovery planning. ❑ Conducts an annual review of mission critical functions and updates recovery and continuity plans.	**LEVEL 4: Optimized**	❑ Contracts with third party organizations to perform additional cyber forensics beyond the scope of internal capabilities. ❑ Prioritizes continuous improvement as part of its culture.

Cybersecurity Strategy Development Guide

- Focuses on how PUCs engage with utilities on cybersecurity preparedness topics.

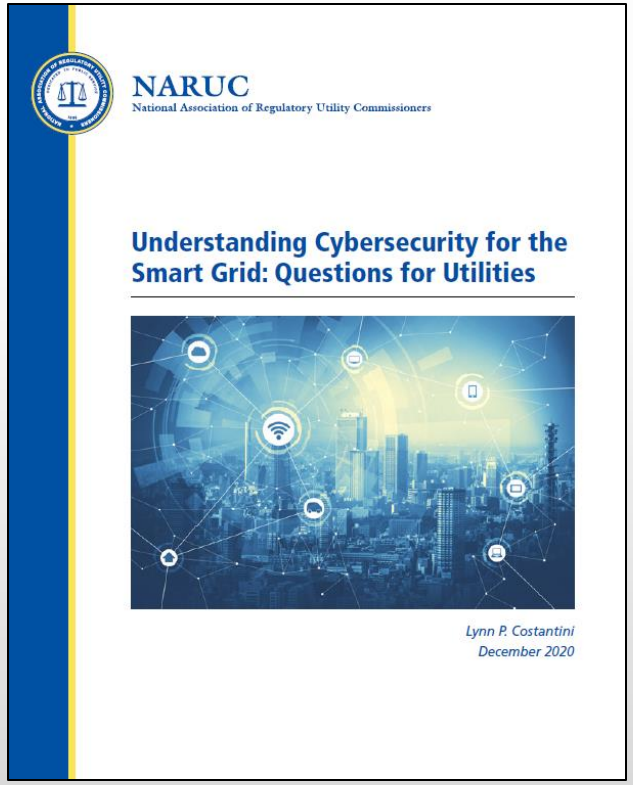
- Provides step by step guidance for developing PUC-specific objectives, goals, and communications plans to ensure meaningful, engagement and actionable outcomes, but may also be applicable for SEO engagement.

Cybersecurity Tabletop Exercise (TTX) Guide



- Guidance to test cybersecurity preparedness and capabilities and **identify areas of success/gaps.**
- Step by step instructions to conduct your own TTX or Seminar, templates included.

Questions for Utilities: Smart Grid



- Discussion prompts for PUCs wishing to explore aspects of utilities' cybersecurity risk management program that target smart grid devices, systems, and networks, collectively referred to as assets
- Leverages NIST Smart Grid Profiles

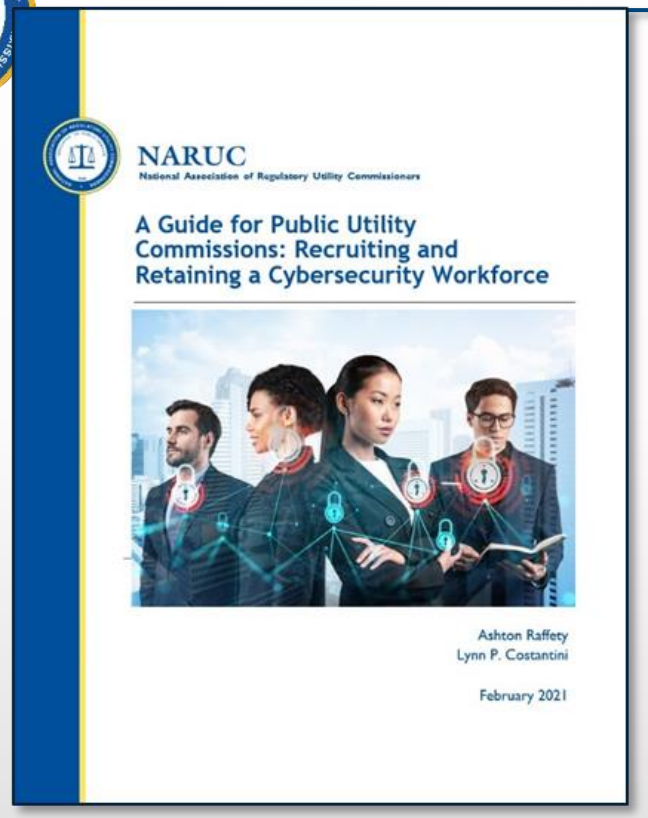
Glossary of Cybersecurity Terms

- Defines cybersecurity terms used in the Cyber Manual plus terms of art PUCs need to know when navigating cybersecurity.

- Builds vocabulary and enhances information sharing.

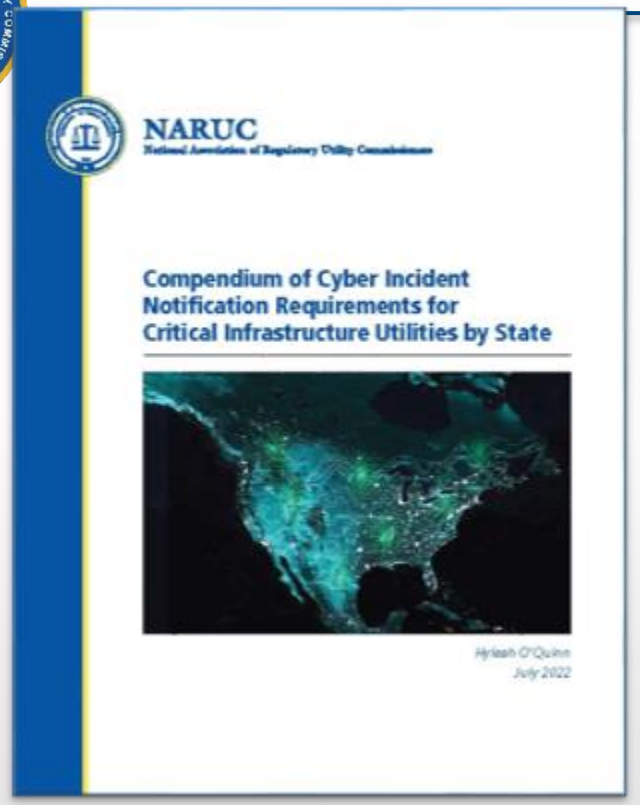
Cybersecurity Incident	**An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.** [1] obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

Cybersecurity Workforce Paper



- Provides insight on cybersecurity roles within PUCs
- Highlights recruitment and retention tactics to expand or develop a cybersecurity division (include alternative tactics)
- Includes a compendium of example cybersecurity job descriptions, pipelines for recruitment, and training opportunities

Cybersecurity Incident Reporting Compendium



- Cybersecurity incident reporting requirements applicable to critical infrastructure utilities (energy, water, telecommunications, etc.) issued by PUCs, state legislatures, or other state agencies.
- State x State
- Does not include PII reporting requirements

Coming Soon…

- On demand user training module for Questions and CPET
- Cybersecurity Baselines for Electric Distribution Utilities

- Also, watch for:
  - Single issue, 1-2 page cybersecurity briefing papers
  - Focus on emergent, high-profile issues to enable PUCs to engage in timely, productive conversations with utilities about mitigation strategies and tactics.

Thank you!

Jody Raines
Sr. Cybersecurity Policy Specialist
Center for Partnership and Innovation
National Association of Regulatory Utility Commissioners
jraines@naruc.org
202.898.8083