NARUC
National Association of Regulatory Utility Commissioners

Cybersecurity Tabletop Exercise Guide

Lynn P. Costantini
Ashton Raffety

September 2020

Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000818.

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.

Acknowledgments

The authors wish to thank the following individuals for contributing their time and expertise to the development of this guide:

- David Alexander, Pennsylvania Public Utility Commission
- Chuck Bondurant, Public Utility Commission of Texas
- Wei Chen Lin, Illinois Commerce Commission
- Daniel Searfoorce, Pennsylvania Public Utility Commission
- Andreas Thanos, Massachusetts Department of Public Utilities
- Kate Marks, Brandi Martin, Brian Marko, U.S. Department of Energy
- Sarah Scafidi and John Ransom, Cadmus Group, LLC

Preface

NARUC developed the Cybersecurity Manual, a comprehensive suite of cybersecurity tools, to help public utility commissions (PUCs) gather and evaluate information from utilities about their cybersecurity risk management and preparedness. These evaluations facilitate well-informed commission decisions regarding the effectiveness of utilities' cybersecurity policies, practices, and related expenditures. This ***Cybersecurity Tabletop Exercise Guide*** is one of five tools in the Cybersecurity Manual.

A brief description of each tool in the Cybersecurity Manual follows:

1. **Cybersecurity Strategy Development Guide**

   The *Strategy Development Guide* defines a road map 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 the drivers of successful outcomes. (2018)

2. **Understanding Cybersecurity Preparedness: Questions for Utilities**

   The *Questions for Utilities* provides a set of comprehensive, context-sensitive questions that PUCs can ask 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 previous NARUC publications. (2019)

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

   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. (2019)

4. **Cybersecurity Tabletop Exercise (TTX) Guide**

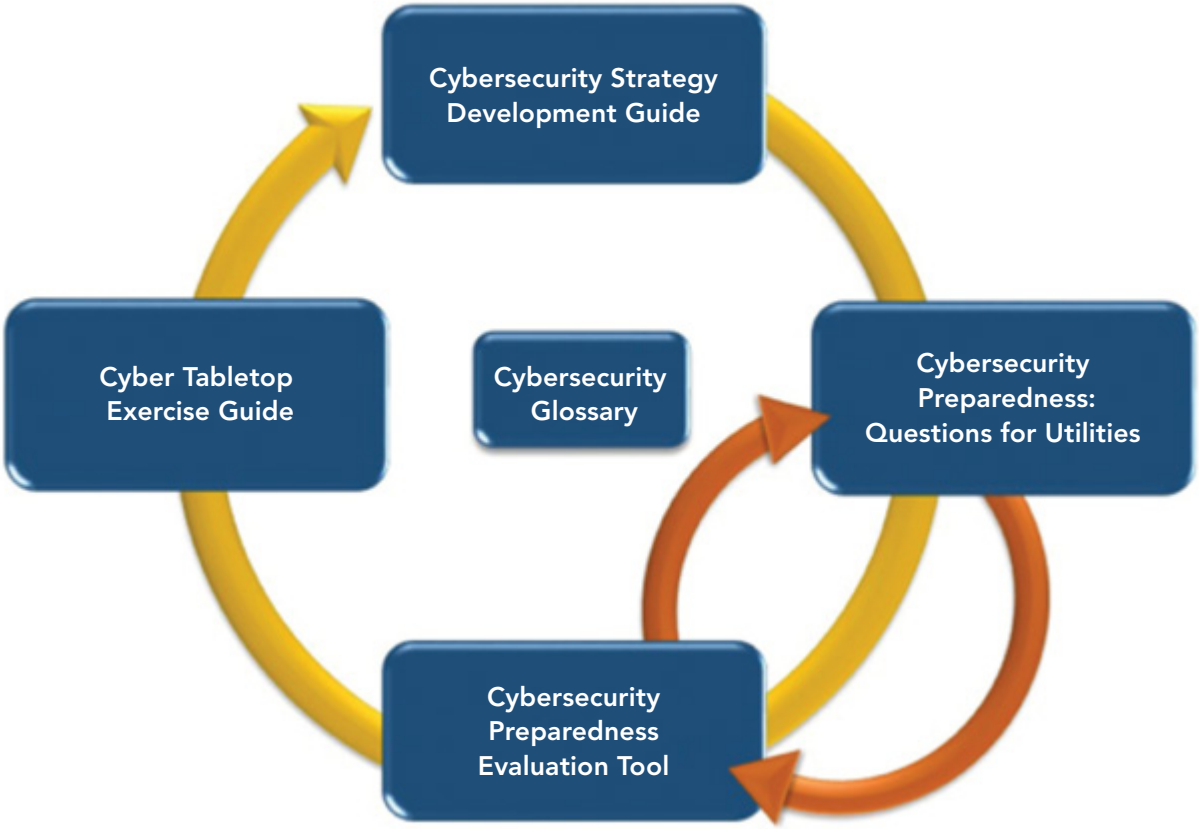
   This guide details the steps that PUCs can take to design and execute an exercise to examine utilities' and other stakeholders' readiness to respond to and recover from a cybersecurity incident. The guide also is helpful to PUCs seeking to exercise their own cybersecurity strategies and capabilities. Exercise scenarios and examples are included. (2020)

5. **Cybersecurity Glossary**

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

Components of 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.

Figure 1. NARUC Cybersecurity Manual Components



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

Table of Contents

Introduction

Public utility commissions (PUCs) are responsible for ensuring adequate, safe, and reliable utility services at reasonable rates. As such, they need to know that jurisdictional utilities' cybersecurity risk management plans and practices—put in place to mitigate cybersecurity vulnerabilities, counter malicious cyber threats, and rapidly respond and recover from successful attacks—are comprehensive and effective. Exercises are useful for this purpose.

Exercises provide opportunities for participants to demonstrate and assess capabilities in specific areas of interest, including cybersecurity risk management. They also facilitate coordination and help clarify organizational roles and responsibilities.

This *Tabletop Exercise (TTX) Guide* steps PUCs through the process of creating and executing an exercise specifically designed to examine capacities and capabilities to plan for, respond to, and recover from a cybersecurity incident involving critical energy infrastructure. It complements other resources in NARUC's Cybersecurity Manual, particularly *Understanding Cybersecurity Preparedness: Questions for Utilities*, and the *Cybersecurity Preparedness Evaluation Tool*.[1] Coupled with the *TTX Guide*, these tools comprise a structured, process-driven approach to identifying, assessing, and testing the efficacy of utilities' cyber risk management plans and practices. This knowledge helps commissions identify cybersecurity gaps, spur utilities' adoption of additional mitigation and response strategies, and encourage improvements.

Part I details the steps to plan and execute a TTX. Part II reviews the steps required to conduct a seminar-based exercise.[2] TTXs are discussion based, typically led by a facilitator who guides participants through one or more scenarios for the purpose of testing the thoroughness and efficacy of relevant plans, processes, and procedures. This format is well suited for commissions' objective assessment of utilities' cybersecurity preparedness as well as their own cyber incident response capabilities. Seminars, which are also discussion-based exercises, typically examine a single procedure within a larger plan or a single step in a multistep process.

Benefits of Cybersecurity Exercises

Rapidly evolving cybersecurity threats and vulnerabilities pose a serious risk to the reliability and resilience of energy infrastructure. The plans, processes, and requisite coordination to manage that risk effectively can be complex and involve numerous internal and external stakeholders. Exercises are the means to bring those stakeholders together in non-crisis environments to ensure preparedness efforts are robust and on target and that response and recovery plans are realistic and well-coordinated. Thus, exercises comprise an integral step in the broader preparedness process.

Some tangible benefits of exercises include the following:

- generate new ideas to solve knotty problems;
- validate planning assumptions and priorities;
- identify resource constraints to meet risk mitigation goals and incident response objectives;
- examine plans, processes, and procedures for relevance and gaps;
- clarify roles and responsibilities before, during, and after an incident;
- assess the compatibility of communications protocols and technologies; and
- enhance training through practice.

---

1 NARUC Cybersecurity Manual: https://www.naruc.org/cpi-1/critical-infrastructure-cybersecurity-and-resilience/cybersecurity/cybersecurity-manual/

2 The steps in each part are based on the U.S. Department of Homeland Security's (DHS) Homeland Security Exercise and Evaluation Program (HSEEP): https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

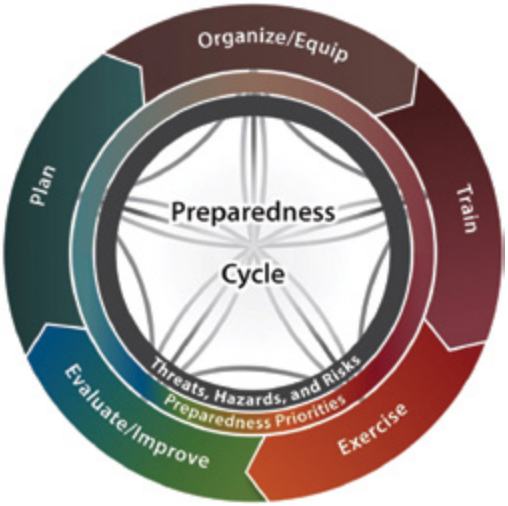
Exercises also provide intangible benefits. Participants often find that exercises help to:

- foster new-found appreciation of others' strengths and weaknesses;
- challenge the status quo;
- improve organizational and individual outlooks and attitudes toward preparedness;
- build deep working relationships with peers; and
- promote cooperative behaviors.

These tangible and intangible benefits translate to better overall stakeholder preparedness, which in turn, may accelerate response to real-world incidents, thereby lessening the deleterious impacts.

By designing and conducting cybersecurity exercises, PUCs are uniquely positioned to explore mechanisms that promote these benefits and build overall awareness and visibility of cybersecurity preparedness and resilience across the utility landscape within their states.

Figure 2. Preparedness Cycle



Source: Homeland Security Exercise and Evaluation Program (HSEEP)

Types of Exercises

A variety of exercise formats exist, from small-scale, discussion-based events to sophisticated, immersive experiences. The level of effort, planning timeframes, and expense to build and deliver an exercise is commensurate with the exercise scope and objectives. Generally, the more sophisticated the exercise, the broader the scope and objectives, the longer the planning horizon. A full-scale exercise (FSE) could take multiple years to successfully plan while an in-person TTX could be designed in as little as six months, although more planning time is suggested. A seminar could be organized in less than three months.

There are two general categories of exercises: discussion-based and operations-based. Discussion-based exercises bring participants together in low-stress environments to talk about their existing plans, processes, and response capabilities, usually in reference to a hypothetical scenario. Designing a discussion-based cybersecurity exercise is not overly burdensome and does not necessarily require specialized cybersecurity knowledge. Conversely, operations-based exercises are high stress and resource intensive. They usually require participants to mobilize to a simulated event in real time using real equipment. The focus of operations-based exercises is practice, skills development, and coordination of effort.

Several different exercise formats exist within each category. For reference, each format is described below.

Discussion-based Exercises:[3]

- **Seminar**—Seminars are lecture-based exercises that orient participants to provide an overview of a strategy, plan, policy, or procedure. Seminars are especially useful when an entity has developed a new plan or made changes to existing plans or procedures.
- **Workshop**—Typically small-group, interactive exercises that focus on idea generation or validation. Built around in-depth, issue-driven discussions, workshops encourage collaboration and joint decision making, which are essential to obtaining consensus and producing effective plans and procedures.
- **Tabletop Exercise (TTX)**—TTXs bring key stakeholders together to work through a scenario for the purpose of testing preplanned actions. This format facilitates a holistic view of strategies and tactics, and allows participants to assess sufficiency and effectiveness, identify gaps, and suggest improvements.

3 FEMA IS-120.C: https://emilms.fema.gov/is_0120c/groups/41.html

Usually, a skilled facilitator guides the discussion to keep participants focused on exercise objectives and may introduce new challenges for participants to address as the scenario unfolds.

- **Game**—Games provide a simulation of operations that often involves two or more teams (e.g., red team/blue team), usually in a competitive environment, using rules, data, and procedures designed to depict an actual or hypothetical situation. These exercises are useful for identifying key operational decision points and exploring the consequences of decisions on play, which help to refine plans and procedures. The informal, low-pressure environment encourages creative problem solving.

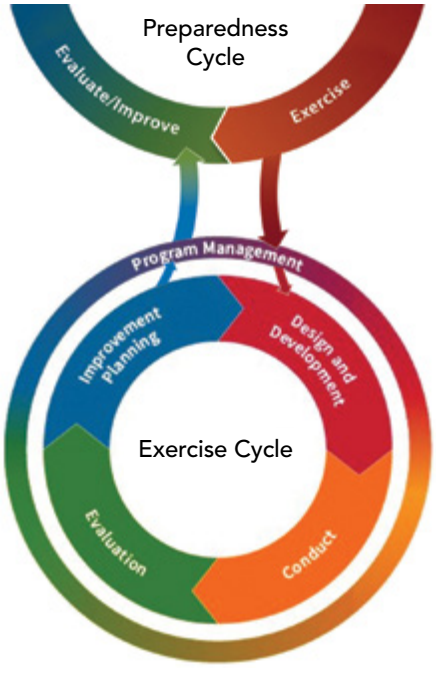
Operations-based Exercises:[4]

- **Drill**—A drill is a coordinated, supervised activity usually employed to validate a specific function or capability in a single organization. Drills are commonly used to provide training on tasks specific to new equipment or procedures, to introduce or validate procedures, or to practice and maintain current skills.
- **Functional Exercise (FE)**—FEs are designed to validate and evaluate capabilities, multiple functions and/or sub-functions, or interdependent groups of functions. FEs are typically focused on exercising plans, policies, procedures, and staff members involved in management, direction, command, and control functions.
- **Full-Scale Exercise (FSE)**—FSEs are high-stress, multi-stakeholder, multi-jurisdictional "boots on the ground" simulations designed to test coordinated responses and rapid problem-solving skills in real time. They involve the actual mobilization of resources across multiple locations. These are the most complex, resource-intensive form of exercises.

Part I: Designing a Cybersecurity TTX

Part I covers the planning, designing, and execution of a cyber TTX. The guide intends to be straightforward but flexible to allow commissions to customize an exercise based on their programmatic goals. During a TTX, participants convene and work through a simulated event to test their response capabilities. Steps outlined throughout this guide intend to help commissions conceptualize the Exercise Cycle.

Figure 3. Exercise Cycle



Source: Homeland Security Exercise and Evaluation Program (HSEEP)

An extension of the Preparedness Cycle (*Figure 2*), the Exercise Cycle (*Figure 3*) depicts the continuous learning that naturally occurs when planning and conducting an exercise. Within an organization's exercise program, there is an endless cycle of designing and developing, conducting, evaluating, and improving exercises and emergency response capabilities. Each step of the cycle is influenced by the preceding step and influences the following. After an exercise is considered complete, the findings and lessons learned, captured in the After Action Report/Improvement Plan (AAR/IP), inform the design and development of the next exercise.

Step 1: Pre-planning Considerations

Before beginning the planning process, commissions may wish to consider the various sources that they can access for exercise planning support as well as potential support for materials and typical exercise amenities (e.g., meals, bottled water, break snacks, etc.). Resources and considerations that commissions should consider before undertaking an exercise include funding opportunities and collaboration with other state agencies, utilities, or other relevant organizations. While funding

4 FEMA IS-120.C: https://emilms.fema.gov/IS0120c/groups/44.html

opportunities are useful, a successful Cyber TTX does not require any special equipment or resources and can be accomplished with zero funding. A TTX could be completed by utilizing existing conferencing space and inviting a small number of key partners to participate.

Planning Support Partners and Opportunities

Cyber TTXs can range in scope, but they are still scalable based on whatever resources (mainly staff time) the PUC may have, and the available planning support from other stakeholders. Individual states may have access to resources and funding for use by their respective commissions. Available funding could be utilized to hire professional assistance, such as facilitators, evaluators, scribes, cybersecurity subject matter experts (SMEs), or secure an off-site venue. An extended list of funding and support opportunities are listed in Appendix G.

Step 2: Identify Objectives

An overview of the planning considerations commissions should keep in mind when identifying exercise objectives.

Exercise Objectives

After completing the preplanning process, a commission can move into the planning portion of the exercise. This begins with the selection of objectives for the cyber TTX, which should focus on the core capabilities specific to the needs of PUCs during a cyber event (i.e., focus on what the PUC wants to test). Objectives may be informed by the commission's cybersecurity strategy or past cybersecurity incidents. Three strong objectives would be a reasonable number to test during a simple half-day TTX. Because commissions face different realities and have varying priorities and resources, each commission benefits from tailoring objectives according to their cybersecurity strategy.[5]

Topical areas for objectives include, but are not limited to, the following:

- Public Affairs
- Information Sharing
- Situational Awareness
- Supporting Service Restoration
- Supporting Recovery
- Supporting State Emergency Response

The commission may also want to consider making the objectives "SMART", meaning specific, measurable, achievable, relevant, and time-bound. Each guideline is defined below.[6]

SMART Guidelines for Exercise Objectives	
Specific	Objectives should address the five Ws: who, what, when, where, and why. The objective specifies what needs to be done with a timeline for completion.
Measurable	Objectives should include numeric or descriptive measures that define quantity, quality, cost, and so on. Their focus should be on observable actions and outcomes.
Achievable	Objectives should be within the control, influence, and resources of exercise play and participant actions.
Relevant	Objectives should be instrumental to the mission of the organization and link to its goals or strategic intent.
Time-Bound	A specified and reasonable timeframe should be incorporated into all objectives.

5 If your commission does not have a cybersecurity strategy, NARUC's recently published Cybersecurity Strategy Development Guide can be used to develop one. If your commission has cyber response plans, or is part of the state's cyber response plan or Cyber Annex, objectives may include testing specific portions or expectations within those plans. Cybersecurity Strategy Development Guide: https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204

6 IS-120.C: An Introduction to Exercises: https://emilms.fema.gov/IS0120c/groups/84.html

Examples of objectives that fit these criteria include:

- Following notification of a cyber incident on energy infrastructure with physical consequences, identify applicable capabilities, and associated authorities, the PUC can employ in response.
- Throughout the exercise, examine state and federal government roles, responsibilities, authorities, and actions that would be used during a cyber incident and identify gaps (if any).
- Following a cyber incident on energy infrastructure, review the ability of the PUC to utilize state, regional, and national communication networks in a timely manner to coordinate unity of effort and unity of message.

Each of the above objectives identifies specific problems, is measurable (via the usage of evaluators), achievable, relevant to examining responses to a cyber emergency, and defines a time period. By designing objectives to be "SMART", commissions may parse out the significant issues they would like to resolve and turn them into viable objectives. All objectives should be evaluated for success following exercise conduct.

Step 3: Composition of Teams and Stakeholders

For an exercise to be successful, the commission should identify an Exercise Leadership Team who will drive the development of the exercise, stakeholders to participate in the exercise, a Planning Team to validate the design of the exercise, and a Facilitation Team to facilitate exercise conduct.

Exercise Leadership Team: Responsible for overseeing all aspects of the Cyber TTX, from designing scenarios to accomplishing objectives, inviting the appropriate stakeholders, executing the exercise, evaluating the success of the exercise, documenting corrective actions, and managing logistics.

- **Exercise Director**: This may be an individual at the commission who either has a background in cybersecurity, emergency preparedness, exercises, or is simply very passionate about it. This individual serves as the exercise manager, chief planner, and convener. To ensure the exercise planning process is progressing, the Exercise Director can utilize the template Cyber TTX Checklist in Appendix B.
- **Lead Designer:** Creates a Situational Manual and any other content needed for exercise conduct. Content should focus on completing exercise objectives. The lead designer will rely heavily on feedback from the Planning Team (described below). A template Situation Manual (SitMan) is in Appendix C.
- **Lead Evaluator:** Responsible for ensuring notes and observations are recorded throughout the exercise, and providing feedback to the Exercise Leadership Team. Observations inform the creation of an AAR/IP (described below). The Lead Evaluator should reference the template Exercise Evaluation Guide (EEG) in Appendix D and the template Feedback Form at the end of Appendix C.
- **Resource/Logistics Lead:** An individual responsible for obtaining proper venues, equipment, and supplies (food, drinks, notepads, etc.) for exercise conduct, as well as providing support for media equipment throughout the exercise (PowerPoints, videos, conferencing/virtual meeting services). If the exercise is conducted virtually, this individual will need to ensure that someone thoroughly tests the virtual meeting platform and is available for technical issues during the exercise.

The commission may have a different way of delineating exercise leads, but using a leadership team with the above composition will likely be sufficient for the creation of a successful cyber TTX. Depending on the size of the exercise and resource availability, an individual may hold multiple roles identified above, or multiple individuals may serve in each of the roles. For more advanced exercises, a breakdown of additional roles and responsibilities is found within the U.S. Department of Homeland Security's Homeland Security Exercise and Evaluation Program (HSEEP) guide.[7]

7 Homeland Security Exercise and Evaluation Program (HSEEP): https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

Once the Leadership Team is identified, they will be responsible for identifying stakeholders, the Planning Team, and the Facilitation Team.

Stakeholders: The Exercise Leadership Team may want to begin identifying key stakeholders before designing the exercise itself. Stakeholder selection should be based on what groups and organizations the PUC would expect to interact with in the event of a cyber incident. Stakeholders could come from the following groups:

- Key State Officials (State Energy Office, Emergency Management Agency, Governor's Office Representatives, Transportation Agency, Information Technology [IT] Officials, State Homeland Security Office, Fusion Center, National Guard Cyber Unit, State Administration Agency)
- Utility Owners/Operators (electricity, natural gas, petroleum, communications, water, non-regulated utilities)
- Federal Partners (U.S. Department of Energy, DOE (including power administrations), U.S. Department of Homeland Security, Federal Emergency Management Agency, Federal Bureau of Investigation, etc.)
- Non-Governmental Organizations (i.e., the Red Cross, other disaster response groups)
- Key local government officials
- Tribal Nations
- First Responders

A significant component of TTXs is building valuable connections between the public and private sectors, so relationships are proactively established in the event of a real incident. However, commissions should be mindful of inviting too many stakeholders because it could result in a less focused and productive exercise. Finding the balance between too many exercise participants and too few is part of the art of exercise design.

Planning Team: Having established your Exercise Leadership Team and stakeholders, the Exercise Leadership Team can now build a Planning Team for in-depth planning of the exercise. The Planning Team should compose of the Exercise Leadership Team and representatives from stakeholder organizations. Individuals in those groups that have been, or will likely be, involved in response to a real-world cyber incident are important to include on the Planning Team. The size of your Planning Team depends on the number of stakeholders invited to participate. For each external organization invited to participate, at least one individual from that organization should participate on the Planning Team. Other than stakeholder organizations and the Exercise Leadership Team, you may want to include the other individuals from the PUC as necessary, including but not limited to:

- **Internal PUC Departments**
  - Emergency Management
  - Cybersecurity Department
  - IT/Operational Technology (OT)
  - General Counsel
  - Investigation and Enforcement
  - Public Affairs/Communications
  - Policy
  - Audits
  - Consumer Services
  - Human Resources

The Lead Designer (a member of the Exercise Leadership Team) is primarily responsible for the exercise design. The Planning Team's primary role is to advise and validate the development of the exercise scenario/injects and objectives. Typically, the Exercise Leadership Team presents the Planning Team with their ideas during planning meetings (discussed below) and asks for input. Changes are then made based on feedback, informing the design and creation of the cyber TTX.

Facilitation Team: The Leadership Team is responsible for either identifying, hiring, or acting as the Facilitation Team. Throughout exercise conduct, the Facilitation Team leads participants through the exercise experience, including recording notes and collecting information that is used to evaluate whether the exercise objectives were reached.

- **Lead Facilitator:** The primary host of the exercise, this individual is responsible for setting the stage, presenting the exercise scenario, introducing injects and discussion questions, and facilitating conversation between exercise participants. The Lead Facilitator should have experience with exercises or the subject matter area being discussed—though this does not necessitate that the individual be an expert in cybersecurity.
- **Co-Facilitator(s):** The Co-Facilitator(s) assists the Lead Facilitator and may present portions of the scenario along with the Lead Facilitator.
- **Evaluator(s):** Throughout the exercise, evaluators record participant progress on objectives and major discussion points using the Exercise Evaluation Guide (EEG). A template EEG is provided in Appendix D.
- **Scribe:** While Evaluator(s) record notes relevant to addressing the exercise objectives, the Scribe focuses on general notetaking (which is useful for Evaluators post-exercise), including a record of attendees. Note: It may be advisable to have participants discuss and agree in advance, in the planning stages, on what information to record during the exercise, who gets the recordings and reports, and what information ultimately gets shared regarding the exercise.

	Leadership Team	Planning Team	Facilitation Team
Role	Responsible for overseeing all aspects of the Cyber TTX, from designing scenarios to accomplishing objectives, inviting the appropriate stakeholders, executing the exercise, evaluating the success of the exercise, documenting corrective actions, and managing logistics.	Convened by the Leadership Team, the Planning Team's primary role is to advise and validate the development of the exercise scenario/injects and objectives. The Planning Team may suggest additional stakeholder groups as the scenario is developed.	Throughout exercise conduct, the Facilitation Team leads participants through the exercise by setting the stage and facilitating discussion. The team also records notes and collects information that is used to evaluate whether the exercise objectives are reached.
Team Composition	• Exercise Director • Lead Designer • Lead Evaluator • Resources/Logistics Lead	• Leadership Team • Representatives from stakeholder organizations • Relevant individuals from the PUC • Lead Facilitator from Facilitation Team	• Lead Facilitator • Co-Facilitator(s) • Evaluators • Scribe *Leadership Team may act as the Facilitation Team
Selected By	Commissioners or PUC Leadership	Leadership Team and Stakeholder Organizations	Leadership Team

Step 4: Select Scenario Type

Once the commission has established the Leadership Team and their objectives for the exercise, the Leadership Team can begin identifying the type of scenario they would like to conduct. The scenario should address the needs of the objectives and form the basis for future design efforts. As the planning process continues, the scenario likely evolves as it becomes more refined. The scenario foundation should include the type of incident(s) that will occur, and determine whether it is a cyber attack against the PUC itself, or involve the PUC responding to a cyber attack that affects utilities within its jurisdiction.

Types of Cybersecurity Scenarios

Commissions deal with a variety of cybersecurity incidents, so many plausible scenarios may be used to gauge cybersecurity readiness across the spectrum. A scenario should be chosen based on what a commission is testing—which could be the PUCs' response, others' response, coordination between entities, preparedness activities, and so on. See different scenario types below.[8] (Scenario examples are listed in Appendix A.)

- **Compromise of Personally Identifiable Information (PII):** Any breach or theft of data that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
- **An Attack on IT/OT Systems of the Utility or PUC:** An attack on critical physical devices that causes utility service disruptions or theft of confidential commission information via a remote hack by an outside actor. An attack aimed at disrupting utility services could also incorporate coordinated cyber and physical attack components.
- **Ransomware Attack:** An attack that occurs from the installation of malicious software on computer hardware. This could occur at the commission or a utility in the PUC's jurisdiction and typically results in information/systems being locked and inaccessible to its usual user. The party responsible for the hack usually demands financial compensation before unlocking information.
- **Cyber Attack on Key Vendors in the Public Utility Commission's Jurisdiction:** The importance of supply chain cybersecurity has grown with the introduction of smart technology into many grid-connected devices. Without proper and regular patching, these devices can become prone to cyber attacks by leaving vulnerabilities open. Malicious software can also be placed in smart grid-connected devices during production, resulting in the theft of personal information. Both would require a response from the utility, PUC, and possibly the governor's office, depending on the severity of the attack.

Commissions can use any combination of the above examples or other cybersecurity-related threats to test response capabilities. The nature and scale of the incident determines which stakeholders should be included in the Planning Team. If it is the commission's first time conducting a cyber TTX, consider beginning with one major incident and then update and refine your TTX to reflect your commission's progress on meeting that exercise's objectives.

Step 5: Establish a Meeting Schedule

The Exercise Leadership Team should create a schedule of meetings for the Planning Team and distribute invitations (or calendar holds) far in advance. This allows members of the Planning Team to prepare and accommodate the planning sessions into their own schedules. A sample meeting schedule is outlined below.

Exercise Planning Meetings

- **Initial Planning Meeting (IPM):** This is the meeting where objectives are discussed and finalized based on feedback from the Planning Team. The Leadership Team's Lead Designer introduces the general scenario and asks for feedback to ensure that the scenario is realistic and applicable to a cybersecurity incident.

  During this meeting, the Exercise Leads should ask for input on who should participate in the exercise from the Planning Team. Participant selection can continue after this meeting, but PUCs may need to be mindful of having too many participants in the planning process.

  - Timeline: Three Months Before Exercise[9]
  - Participants: Exercise Leadership Team/Planning Team/Facilitation Team

8 Many of the terms above are defined in NARUC's Cybersecurity Glossary: https://pubs.naruc.org/pub/7932B897-CF16-0368-BF79-EDC5C5A375EE

9 Timing for each meeting depends on the size and scope of the exercise. Timelines are suggestions.

- **Midterm Planning Meeting (MPM):** The MPM may involve a more in-depth examination of the exercise scenario. This could include formulating the exercise injects, reviewing cyber incident response plans, and reviewing a draft version of the SitMan developed by the Lead Designer. The SitMan details the events that occur during the exercise.
  - Timeline: Two Months Before Exercise
  - Participants: Exercise Leadership Team/Planning Team/Facilitation Team
- **Final Planning Meeting (FPM):** The FPM is the final meeting of the TTX planning process. During this meeting, the Exercise Leadership Team asks for feedback from the Planning Team on all draft documents used to drive exercise play. Final changes to the scenario should be complete before the FPM so edits can be discussed and agreed upon during the FPM. At this meeting, the Resource/Logistics Lead confirms any outstanding logistical issues.
  - Timeline: One Month Before Exercise
  - Participants: Exercise Leadership Team/Planning Team/Facilitation Team

Commissions should note that a great deal of the discussion concerning exercise design topics can occur in between the above meetings. The suggestions above are meant to serve as guideposts for commissions. It may be necessary for the Planning Team to meet more frequently as exercise design is an iterative process.

Step 6: Exercise Design

This section focuses on how to design activities for the cyber TTX. The process that each commission goes through likely varies depending on the commission's size and available resources.

Review Plans

A review of cyber emergency plans may occur earlier on in the process when the Exercise Leadership Team is designing their objectives and goals for the scenario. Still, it is a vital part of exercise design. Planners should review all relevant plans and policies related to incident response, recovery, or other activities to be explored in the scenario. Relevant plans include internal PUC procedures and stakeholder plans that would help drive exercise play. By reviewing cyber incident response and recovery plans, the Planning Team has an understanding of how the response structure for a cyber emergency is supposed to work, which provides valuable information on what capabilities should be tested during the TTX. Evaluators begin shaping the criteria on which they evaluate the exercise based on the plans or procedures utilized during exercise conduct.

Development of Basic Scenario Elements

When designing a scenario, the Planning Team may want to keep the following three elements in mind:[10]

- The conditions allowing players to demonstrate their ability to meet exercise objectives;
- The technical details necessary to accurately depict scenario conditions and events (e.g., the date and time of event and damage resulting from the event); and
- A general context or comprehensive narrative.

While developing the scenario, everyone should keep the above elements in mind, as well as what sort of disruptive elements participants experience during the scenario. All of these elements should be developed by the Exercise Leadership Team and presented at the IPM, where feedback should be collected from the Planning Team. Example scenarios are in Appendix E.

10 HSEEP, p. 3–12: https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

Scenario Injects

"Modules" typically represent a specific period in the overall scenario (e.g., pre-event, post-incident, the morning of the event, etc.) while "injects" represent a new development or incident that builds the overall scenario. Injects are typically included within modules (e.g., Scenario > Modules > Injects). More advanced exercises can contain this level of depth. This guide focuses on developing simple TTXs, so for simplicity, we focus on developing injects beneath the broader exercise scenario (e.g., Scenario > Injects).

The elements or information introduced in each inject should complement the commission's exercise objectives and the core capabilities that it would like to see tested. Following each inject, a facilitator typically asks discussion questions to drive participants toward the core items within the exercise objectives. Example scenarios, injects, and discussion questions are in Appendix A.

Create Situation Manual

Before the MPM, you may wish to develop a SitMan that details the events that occur in the scenario as well as any pre-reading materials deemed necessary for successful participation in the exercise. The SitMan length varies depending on the complexity of the scenario and what objectives the commission would like to test. A SitMan typically includes an introduction that provides a broad overview of the exercise scope, objectives, rules (including safety instructions), assumptions, and structure of the exercise.[11] The section following the introduction contains a description of the scenario and injects with discussion questions. Appendices of the SitMan may include the commission's cyber incident response plan (if applicable), contact information of exercise participants, and a glossary of terms. A broad outline of what your commission may want to include in the SitMan is listed below. A template SitMan is in Appendix C.

- Handling Instructions
- Safety Instructions
- Schedule/Agenda of the Exercise
- Exercise scope and objectives
- List of Participants
- Exercise Structure, Guidelines, and Assumptions
- Scenario and Injects (w/ discussion prompts)
- Participants Feedback Form
- Acronym List

Development of EEG

During the exercise, the Lead Evaluator evaluates whether objectives have been accomplished. Commissions may want evaluators to develop an EEG to ensure that the PUC is meeting its goals and staying on track with its objectives throughout the exercise design process. EEGs accomplish the following:[12]

- Streamline data collection during the exercise (consider sensitive information and how to avoid bringing it into the exercise or protecting it if deemed critical);
- Enable thorough assessments of the participant organizations' capability targets;
- Support development of the AAR/IP following the exercise;
- Provide a consistent process for assessing preparedness through exercises; and
- Help organizations map exercise results to exercise objectives, core capabilities, capability targets, and critical tasks for further analysis and assessment.

There may be a variety of ways to meet all of these above targets, and they likely vary based on each commission's goals and priorities. It may be useful to apply SMART principles to each of the above bullets

11 HSEEP, p. 3–13: https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

12 HSEEP, p. 5–4: https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

to ensure that evaluation can occur effectively. By referring back to the SMART framework, commissions may be able to help evaluators better frame the EEGs and narrow their focus to improve their effectiveness. See a template EEG in Appendix D.

Step 7: Exercise Conduct

Once the design is complete, it is time to conduct the exercise. This portion covers what sort of materials (and staff) may be required to facilitate the exercise, the pre-reading materials that commissions may wish to provide participants, as well as inspection of the venue space before exercise conduct.

Exercise Venue

A Cyber TTX should follow standard practice for meeting logistics. For example, consider venue size, food, and refreshments required, as well as ensuring breaks are scheduled to encourage networking and discussion. It is important to choose a venue that has space for all participants, staff, and observers to move about and have separate discussions without noise becoming a distraction. For more advanced exercises, it may also be useful to have smaller breakout rooms where participants can have more in-depth conversations concerning the exercise or to network with one another.

An in-person Cyber TTX should not require any special equipment or materials since it is a discussion-based exercise. Concerning equipment, audio/video capabilities to display a slide deck or video will likely be the only equipment needed. Video telecommunication abilities may be needed if some individuals join the TTX remotely. Before the exercise, the Leadership Team should visit the venue space to ensure bathrooms and emergency exit locations are known and clearly labeled for participants (create signage if necessary). An initial run of the entire exercise may also be useful to address any problems that occur.

If the TTX is conducted virtually or with a remote play option, a conferencing system or virtual meeting software is necessary. The chosen platform should be thoroughly tested before the exercise, including all features that may confuse a non-expert user. To ensure that the TTX runs smoothly, someone should be responsible for addressing technical issues if they arise during the exercise.

Pre-reading Materials

To facilitate active participation in the exercise, provide pre-reading materials to participants to ensure that all players start with an equal base-level of knowledge. Reading materials beforehand allows them to focus on building relationships through interactions, rather than passively reading during exercise conduct. Pre-reading materials could include:

1. Logistical information (parking instructions, building access instructions, dress code, etc.)
2. The Situation Manual (SitMan)
3. Your State's Energy Assurance Plan, State Emergency Operations Plan, and/or Cyber Emergency Response Annex
4. Brief biographies of the Exercise Facilitator(s), Evaluators, and Scribe (and Exercise Leadership Team if different).
5. Previously developed energy risk profiles of the state/region[13]
6. PowerPoint used during the exercise (if applicable)
7. Copies of the EEG should be sent to evaluators before exercise conduct.

13 State and Regional Energy Risk Assessment Initiative: https://www.energy.gov/ceser/state-and-regional-energy-risk-assessment-initiative

Executing the Exercise and the Evaluator's Role

Once the exercise has begun, the Lead Facilitator may ask all participants to introduce themselves to help participants think about how they can interact with one another during the exercise and an actual emergency. Following introductions, the Lead Facilitator can provide an overview of the scenario and begin exercise play. During the exercise, evaluators can observe the participants' decision-making processes, record actions, and collect exercise data. Possible actions to observe include:[14]

- Plans, policies, and procedures referenced or followed during the exercise;
- Interdepartmental authorities used or implemented;
- Roles and responsibilities of the commission, participants, and any other organizations involved;
- Significant decisions made, including information gathered to make decisions;
- Thresholds discussed (e.g., if "X" happens we suggest "Y" to the governor);
- Activation or implementation of processes and procedures, requests for resources, use of coordinated cyber incident response plans, etc.;
- How and what information was shared with other agencies/organizations and the public; and
- Gaps or questions asked without resolution.

Hot Wash

Immediately following completion of the exercise, the Exercise Team can hold a "Hot Wash". A Hot Wash allows participants to provide feedback on how they thought the exercise progressed and how they performed. Exercise strengths and areas that may need improvement are usually also discussed during this session. The Hot Wash may be led by the Lead Facilitator, who ensures that discussion points remain on topic and relevant to the objectives and goals laid out by the commission at the beginning of the exercise. Evaluators may use the information collected from the Hot Wash to inform the AAR/IP. The Hot Wash likely provides the Exercise Leadership Team with ideas to improve subsequent exercises. A template Hot Wash Discussion Form for evaluators to utilize is included in the template EEG (Appendix D).

Discussion and Follow-Up

Following exercise completion and the Hot Wash, the Exercise Leadership Team discusses possible next steps to improve their capabilities. The commission may also consider including a mechanism (such as a survey or feedback form) for collecting anonymous feedback from the participants to help improve the exercise and determine the usefulness/value of exercise to participants. At a later date, the Exercise Leadership Team should reconvene with evaluators to discuss outcomes and determine whether the exercise objectives were achieved. The Exercise Team may wish to send a follow-up email shortly after the exercise to thank participants for attending. The email may also include a note that information on the AAR/IP and After Action Meeting (AAM) is forthcoming.

Step 8: Evaluation

The first evaluation takes place in the form of a Hot Wash immediately after the exercise. At a later date, the Exercise Leadership Team and Facilitation Team debriefs among themselves to determine whether the exercise objectives were accomplished. If necessary, a data analysis phase takes place, then an AAR/IP is developed and validated through an AAM.

Data Analysis

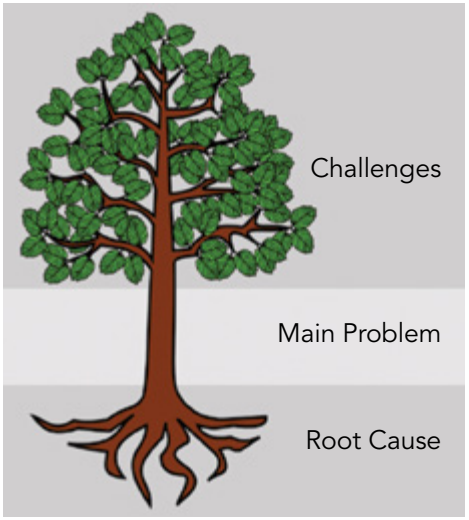
During the analysis phase, evaluators and the Scribe consolidate data collected during and after the exercise to identify strengths, challenges, and other observations to determine if the exercise objectives were met. Evaluators can conduct this task by finding the root cause or origin of each challenge. This is known as Root Cause

14 HSEEP, p. 5–4: https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

Analysis (*Figure 4*) and typically involves the evaluator attempting to trace the underpinnings of each challenge. By examining the chain of events, the evaluator may be able to find what ultimately prevented the critical function from occurring. Some questions that evaluators may need to ask themselves include the following:[15]

- Were the commission's objectives achieved?
  - If not, what factors contributed to this result?
- What was supposed to happen based on current plans, policies, and procedures?
  - Was that what occurred?
  - Were the consequences of the action (or inaction/ decision) taken positive, negative, or neutral?

Figure 4. Root Cause Analysis



Step 9: Improvement Planning

After-Action Report/Improvement Plan (AAR/IP)

Following the completion of data analysis, the Exercise Leadership Team (and possibly Facilitation Team) may begin drafting an AAR/IP. This document typically includes an overview of the exercise scenario/modules, a list of participating organizations, a description of the objectives tested, and a list of corrective actions. The Exercise Leadership Team may also wish to include an overview of participant's performance based on the commission's goals and objectives. This may be expanded to include the participant's strengths and areas of improvement for each exercise objective.

The document typically includes corrective actions, which are actionable, achievable, and identify a responsible party and completion date. Corrective actions form the backbone of this process and highlight ways that commissions can improve their response to various forms of cyber emergencies.

Although not exhaustive, the Exercise Leadership Team may wish to use the following questions during discussions on developing corrective actions:[16]

- What changes need to be made to plans and procedures to improve performance?
- What changes need to be made to organizational structures to improve performance?
- What changes need to be made to management processes to improve performance?
- What changes to equipment or resources are needed to improve performance?
- What training is needed to improve performance?
- What are the lessons learned for approaching similar problems in the future?
- What changes need to be made to the exercise itself?

15 HSEEP, p. 5–8: https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

16 Expanded based on HSEEP, p. 6-2: https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

Example Corrective Action:

- Energy assurance plans should provide more detailed plans and approaches for dealing with cyber incidents, and should include the roles and responsibilities of all the state agencies that could be involved in the responses and public messaging. States should be prepared to identify what planning, policy, and regulatory actions have already taken place, and align them with Presidential Policy Directive (PPD)-41.
    - **Responsible Party:** [Insert Responsible Party]
    - **Completion Date:** [Insert Date]

Once the AAR/IP is drafted, it can be distributed to the Planning Team (and possibly other stakeholders) for review before the AAM.

> **Note:** Caution should be taken regarding the evaluation and the possible identification of risks, weaknesses, and response plan shortcomings. Each organization may be assigned different responsibilities for addressing any such discoveries. However, commissions may want to be mindful of releasing any of these weaknesses into the public via the AAR/IP. Malicious actors could potentially capitalize on vulnerabilities identified within the AAR/IP.

After-Action Meeting (AAM)

AAM's are typically used to review the AAR/IP and finalize findings. During the AAM meeting, discussions should focus on observations, including identified areas of improvement and positive exercise results. By the end of the meeting, the Exercise Leadership Team may try to reach a consensus among the participants on exercise strengths and draft corrective actions. Deadlines for progress on corrective actions may also be discussed during the AAM.

Exercise Completion and Iteration

Once the final copy of the AAR/IP is complete, it can be distributed as widely as appropriate, and exercise is considered complete. However, commissions may need to check in with other participating organizations and ensure that they are meeting their goals to address corrective actions outlined in the AAR/IP. Improvement plans are notorious for sitting a shelf after a lot of effort went into their development. To ensure that progress is continually being made, checking on the status of improvement plans should be an iterative process with support from PUC leadership. Prioritization of continually refining and improving emergency response plans needs to be a priority to see results. As identified in the Exercise Cycle (*Figure 2*), a follow-up exercise may examine whether or not the participating organizations progressed on their corrective action items. The process for exercise design can then begin again.

Part II: Designing a Cybersecurity Seminar

A seminar is a discussion-based exercise that tests an organization's preparedness by working through existing strategies, plans, policies, or procedures with relevant partners. In this case, the objective of a seminar is to ensure that all parties understand their cybersecurity roles and responsibilities. This section of the guide focuses on how a seminar can enhance the cybersecurity posture of utilities by reviewing existing cybersecurity-related documents and finding opportunities to clarify expectations or procedures among critical partners.

Contrasted to a TTX, a seminar is less complicated to plan and conduct. A seminar typically takes place around a conference table with 10 to 15 individuals working through a document and discussing its real-world application, but could include even less or more individuals depending on the type of material reviewed and the number of relevant stakeholders involved.

It is essential to note the difference between a seminar and a workshop. While similar and many professionals use the terms interchangeably, the main difference is the intention of the gathering. While seminars can inform updates to an existing document or plan, the primary purpose is to provide and clarify information and expectations between stakeholders about existing documents and protocols. The primary intention of a workshop is to formally bring stakeholders together to create or edit plans, procedures, or agreements with consensus.

Step 1: Identify Document(s) to Discuss

A PUC and key critical infrastructure partners could utilize the document types outlined below to conduct a seminar.

- **Understanding Cybersecurity Preparedness: Questions for Utilities**[17]
  - Developed and released by NARUC in 2019, this document provides a pathway for formal or informal conversations between a PUC and their regulated utilities about a utility's cybersecurity posture and hygiene. Part II of this document offers 42 questions (plus sub-questions) that could be worked through to provide PUCs with a better understanding of a utility's cybersecurity program.
  - After working through these questions with a utility, you can analyze the information received using NARUC's CPET.[18] The CPET provides commissions with a simple, easy-to-apply tool to evaluate the maturity of a utility's cybersecurity program. By regularly engaging with utilities (e.g., annually, semiannually) using the Questions for Utilities and analyzing the information received using the CPET, commissions can assess the year-over-year change in cybersecurity preparedness of individual utilities. This practice would promote continuous improvement.
  - Participants: PUC/Utilities (one on one)
- **PUC's Cybersecurity Strategy**
  - A cybersecurity strategy enables commissions to understand how their utilities prepare for, respond to, and recover from cybersecurity incidents. It may also assist commissions by identifying additional activities that could minimize cybersecurity risk to electric distribution systems. If your commission does not have a cybersecurity strategy, a workshop may be appropriate to develop one utilizing NARUC's Cybersecurity Strategy Development Guide.[19]
  - Participants: PUC/Utilities/Relevant state agencies

17 Understanding Cybersecurity Preparedness: Questions for Utilities: https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220

18 Cybersecurity Preparedness Evaluation Tool: https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0

19 Cybersecurity Strategy Development Guide: https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204

- **Energy Assurance Plan (EAP)/Cybersecurity Annex**
  - Each state has an EAP that typically delineates the responsibilities of state agencies that either lead, co-lead, or support emergency support function (ESF)-12 (energy). These plans may include a cybersecurity annex, which identifies how emergency coordination will take place in the event of cybersecurity disruptions on the energy sector.
  - Participants: PUC/Utilities/Other state agencies identified in the EAP

Step 2: Identify Stakeholders

Stakeholders for the seminar should include groups and organizations the PUC would expect to interact with when implementing cybersecurity preparedness programs or responding to a cybersecurity incident. Stakeholders could come from the following groups:

- Key State Officials (State Energy Office, Emergency Management Agency, Governor's Office Representatives, Transportation Agency, IT Officials, State Homeland Security Office, Fusion Center, National Guard Cyber Unit, State Administration Agency)
- Utility Owners/Operators (electricity, natural gas, petroleum, communications, water, non-regulated utilities)
- Federal Partners (U.S. Department of Energy (including power administrations), U.S. Department of Homeland Security, Federal Emergency Management Agency, Federal Bureau of Investigation, etc.)
- Non-Governmental Organizations (i.e., the Red Cross, other disaster response groups)
- Key local government officials
- Tribal Nations
- First Responders

Step 3: Seminar Conduct

Conducting a seminar can be as simple as convening five stakeholders for a couple of hours, but typically consists of 10 to 15 individuals assembling for a half day with plenty of networking breaks built into the agenda. Planning for the seminar conduct should follow standard practices for meeting logistics. In-person and virtual meeting considerations should follow suggestions made in Part I: Step 7 of this guide.

Seminar Roles

- **Opening Speaker:** Consider inviting a commissioner or another prominent leader to make brief opening remarks. Opening remarks can highlight the importance of preparation and provide an overview of the seminar's goals. The opening speaker does not need to stay for the duration of the seminar if they are not integral to the conversation.
- **Facilitator:** The seminar facilitator should be someone with authority on the document planned for discussion. This person is responsible for facilitating dialogue and prompting seminar participants when appropriate. Examples:
  - If NARUC's "Questions for Utilities" is discussed, the PUCs Cybersecurity Director may lead the discussion and prompt utilities for additional details as appropriate.
  - If an EAP/Cyber Annex is discussed, the ESF-12 lead may facilitate the discussion and prompt other agencies to describe their cybersecurity roles during an incident.
- **Scribe:** The Scribe should take notes throughout the seminar to capture major discussion items. Notes do not need to be overly detailed and should not identify specific individuals.

Pre-reading Materials

To facilitate active participation in the seminar, provide pre-reading materials to ensure that everyone has the opportunity to review documents and form questions before the seminar. The only required pre-reading material would be the document planned for discussion, but others may include:

1. Logistical information (parking instructions, building access instructions, dress code, etc.)
2. Your State's Energy Assurance Plan, State Emergency Operations Plan, and/or Cyber Emergency Response Annex
3. Brief biographies of key participants
4. Previously developed energy risk profiles of the state/region[20]
5. PowerPoint that will be used (if applicable)

Step 4: Post Seminar Actions

Unlike a TTX, there is no formalized process for evaluating the success of a seminar. Nevertheless, follow-up actions may be taken to improve the strategies, plans, policies, or procedures discussed. Post seminar, a feedback questionnaire can be distributed to participants to identify the clarity of the document discussed. If significant misunderstandings are discovered, a workshop could be convened between stakeholders to formally recommend edits to an existing document or develop an entirely new one.[21]

20 State and Regional Energy Risk Assessment Initiative: https://www.energy.gov/ceser/state-and-regional-energy-risk-assessment-initiative

21 Workshops are more structured than seminars. Participant attendance and collaboration from relevant stakeholders is essential to obtain consensus and produce effective plans, procedures, and agreements.

A. Example Cybersecurity TTX Scenarios and Injects

The example scenarios and injects listed below were previously conducted by PUCs or are heavily based on actual cybersecurity exercises.

1. Ransomware Attack on Commission

Scenario: Orchestrated by an unknown assailant, a ransomware DDOS attack takes place against XYZ Public Utility Commission. There is concern that the attack will spread to utilities if the assailant uses private contact information stored with the commission's network to launch a phishing campaign. However, there is no evidence to suggest that this is the attacker's intent.

- **Inject 1** [9:00 AM]: It is seemingly a typical day at the commission, and operations are running smoothly. However, the PUC's IT department notices a series of abnormal spikes in activity within one of their systems. The peaks are initially dismissed as routine fluctuations, and the day continues as usual.
    - Discussion Question: What protocol or precedence exists for suspicious internal network abnormalities?
- **Inject 2** [12:00 PM]: A few hours later, the commission's website crashes due to a high volume of traffic. The PUC's IT department realizes that the commission is currently under a Distributed Denial of Service (DDOS) attack, explaining the abnormal fluctuations from earlier.
    - Discussion Question: What would the PUCs communications/public affairs department do in this scenario?
- **Inject 3** [3:00 PM]: Three hours after the initial discovery of the DDOS attack, a commission staffer receives an email claiming to be a hacker. The hacker states that they will continue to execute daily DDOS attacks on the commission unless the PUC pays them. To make matters worse, the hacker claims to have access to Personally Identifiable Information (PII) from employees and customers and demand payment. If you do not pay, the hacker threatens to release the PII publicly. The hacker copies members of the press on the email.
    - Discussion Question: What state/federal partners would you contact to help address the situation?

2. Cyber Attack on Regulated Utilities

Scenario: As alerted by a federal agency, malicious cyber actors are seemingly targeting water utilities and taking over their operational systems to release excessive amounts of chlorine into treatment centers.

- **Inject 1** [10:00 AM, June 1]: the FBI issues a Private Industry Notification (PIN), TLP Amber[22], based on information received from several water utilities across the country. The PIN notes that malicious actors are utilizing phishing techniques to send personal emails with files embedded with malware. The actors appear to focus on access to operational systems and SCADA.
    - **Discussion Question:** What is your degree of concern at this point? Are there any actions that need to happen now?
- **Inject 2** [11:00 AM, June 3]: An employee at a private utility water plant opens an email addressed to them from an apparent vendor with a PDF attachment invoice. The employee opens the PDF and deletes the email after viewing the PDF. About an hour later, other plant personnel investigate a strong chlorine smell and determine that an excessive amount of chlorine was released into the treatment system during the disinfection process. However, SCADA and PLCs are not indicating any problems. Plant operators

22 Traffic Light Protocol (TLP) Definitions and Usage: https://www.us-cert.gov/tlp

notify corporate security and IT as well as the State Environmental Agency, per the state requirements. Corporate security notifies DHS CISA and the FBI.

  - **Discussion Question:** Who else should be notified and by whom?

- **Inject 3** [2:00 PM, June 3]: Due to the loss of control of the chlorine feed and control of the SCADA and operations systems, the company shuts the plant down and issues do-not-consume and water conservation notices.

  - **Discussion Question:** If the water company issues a "do-not-consume" notice, what type of public messaging needs to come from which state agency?

- **Inject 4** [4:00 PM, June 3]: A separate water system in another part of the state reports to the state emergency management agency that a successful phishing attack conducted reconnaissance on control systems, but was mitigated by IT staff before it migrated to the control systems.

  - **Discussion Question:** How would this information be shared with other water utilities and other critical infrastructure sectors to warn of a potential threat?

3. Combined Cyber Incident and Workforce Disruption

Scenario: Amid a global health pandemic, a malicious cyber actor targets personally identifiable information (PII) within a regulated utility. The PUC and other state and federal agencies must respond to the cybersecurity incident while following strict health and safety protocols.

The Centers for Disease Control and Prevention (CDC) previously made a public announcement that an unknown and contagious disease is infecting about 1,000 people per day within the United States. The CDC advises citizens to wear protective face masks and avoid public/crowded spaces until further notice. The CDC also recommends that Governors issue shelter-in-place orders to temporarily close restaurants and other public places prone to crowding.

- **Inject 1** [10:00 AM, Friday]: Based on CDC recommendations, XYZ Utility is limiting the number of employees in the office at any given time to 25% capacity, and all other employees are required to work from home. All employees have work laptops.

  - **Discussion Question:** Do protocols/technologies exist for secure remote connections? If so, how are employees trained?

- **Inject 2:** Strains on the utility's remote access network have caused utility employees to become frustrated with loading speeds of their email and other work applications. Many employees start accessing their work emails from their personal computers, not connected to the utility's VPN network. The utility's IT team would usually notice suspicious IP addresses accessing their system. But, due to the unusual work from home rule, they do not limit employees from accessing their work from their personal computers.

  - **Discussion Question:** At any given moment, how many employees can access the network remotely? Do you have the ability to increase this capacity if necessary?

- **Inject 3** [8:00 AM, Monday]: Over the weekend, there was a large number of unusual IP addresses accessing the utility's network, even more so than when employees were utilizing their personal computers. IT then discovered that the PII was accessed and copied by an unauthorized user. The IT department immediately reports this breach to their Chief Information Security Officer (CISO).

  - **Discussion Question:** Is there a protocol for notifying individuals that their PII was compromised?

Appendix B. Template Cyber TTX Checklist

Commission Name:	Name of Exercise:
Exercise Location:	Exercise Date:

Exercise Planning Tasks	Assigned To	Suggested Timeline	Date Completed	Notes
Design and Development				
1. Preplanning Considerations				
Identify funding or support opportunities that could be utilized to conduct a Cyber TTX (Appendix G).	[Commissioners, PUC Leadership, or Exercise Leadership Team]	[7-8 months before the exercise]		
2. Identify Objectives				
Identify exercise purpose and draft objectives. Make the objectives specific, measurable, achievable, relevant, and time-bound (SMART).	[Commissioners, PUC Leadership, or Exercise Leadership Team]	[8 months before the exercise]		
3. Composition of Teams and Stakeholders				
Identify an Exercise Leadership Team to manage all aspects of the exercise.	[Commissioners or PUC Leadership]	[8 months before the exercise]		
Identify key stakeholders based on who PUCs would expect to interact with during a cyber incident.	[Exercise Leadership Team]	[7-8 months before exercise]		
Stand up the Planning Team with individual stakeholders and the Exercise Leadership Team.	[Exercise Leadership Team and Stakeholder Organizations]	[6-7 months before exercise]		
Identify or hire a Facilitation Team.	[Exercise Leadership Team]	[5-7 months before exercise]		

Exercise Planning Tasks	Assigned To	Suggested Timeline	Date Completed	Notes
4. Select Scenario Type				
Identify scenario type and scope.	[Exercise Leadership Team]	[6-7 months before exercise]		
5. Establish a Meeting Schedule				
Draft and send invitations/calendar holds for the IPM, MPM, FPM, and Exercise Date to participants.	[Resource/Logistics Lead]	[4 months before exercise]		
Initial Planning Meeting (IPM) Discuss and finalize objectives based on feedback from the Planning Team. The Leadership Team's Lead Designer will also introduce the general scenario and ask for feedback to ensure that the scenario is realistic and will address problems that may be encountered during an actual cyber emergency.	[Exercise Leadership Team]	[3 months before exercise]		
Midterm Planning Meeting (MPM) The MPM may involve a more in-depth examination of the exercise scenario. This could involve formulating the exercise injects, reviewing cyber incident response plans, and reviewing a draft version of the Situation Manual (SitMan) developed by the Lead Designer. The SitMan will detail the events that will occur during the exercise.	[Exercise Leadership Team]	[2 months before exercise]		

Exercise Planning Tasks	Assigned To	Suggested Timeline	Date Completed	Notes
Final Planning Meeting (FPM) Ask for feedback from the Planning Team following the MPM on all draft documents being used to develop the scenario. Any changes to the scenario are completed before the FPM so that they can be discussed and agreed upon during the FPM. At this meeting, the Resource/Logistics Lead will confirm any outstanding logistical issues.	[Exercise Leadership Team]	[1month before exercise]		
6. Exercise Design				
Review: • Existing cybersecurity plans and procedures • Risk, threat, and hazard assessments specific to the state/region • Relevant After-Action Report/ Improvement Plan (AARs/IPs) from previous exercises or other relevant exercises	[Exercise Leadership Team and Planning Team]	[5-6 months before exercise]		
Develop basic scenario elements and injects (examples in Appendix A).	[Lead Designer]	[Before IPM]		
Create Situation Manual (SitMan) (Appendix C).	[Lead Designer]	[Before MPM]		
Develop Exercise Evaluation Guide (EEG) (Appendix D).	[Lead Evaluator]	[After objectives are finalized SitMan is drafted]		

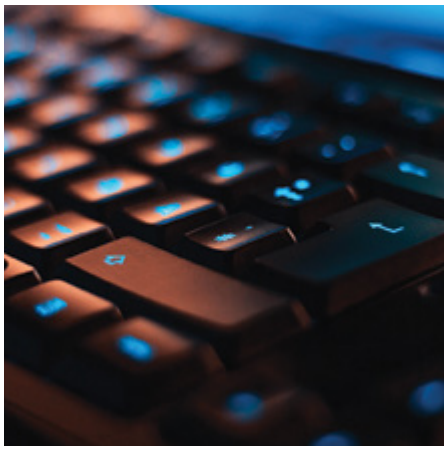
Exercise Planning Tasks	Assigned To	Suggested Timeline	Date Completed	Notes
Develop multimedia exercise presentation (if applicable)	[Facilitation Team or Lead Designer]	[Before FPM]		
Develop Participant Feedback Forms (end of Appendix C).	[Lead Evaluator]	[Before FPM]		
Conduct				
7. Exercise Conduct (and logistics)				
Compile and send Pre-Reading Materials to participants to ensure that all players start with an equal base-level of knowledge.	[Exercise Leadership Team]	[3 weeks before exercise]		
Identify and reserve exercise venue	[Resource/ Logistics Lead]	[5-6 months before exercise]		
Arrange for participant parking at venue	[Resource/ Logistics Lead]	[2 months before exercise]		
Arrange for audio/visual equipment (e.g., microphones, screens, projectors)	[Resource/ Logistics Lead]	[2 months before exercise]		
Arrange for exercise supplies (e.g., pens, markers, flipcharts)	[Resource/ Logistics Lead]	[2 months before exercise]		
Develop ID badges, name/table tents, and sign-in sheets	[Resource/ Logistics Lead]	[1 week before exercise]		
Develop signage (if necessary)	[Resource/ Logistics Lead]	[1 week before exercise]		
Conduct Exercise	[Facilitation Team]	[Day of Exercise]		
Conduct Hot Wash	[Facilitation Team]	[Day of Exercise]		
Determine Follow Up Steps	[Exercise Director]	[Day of Exercise]		

Exercise Planning Tasks	Assigned To	Suggested Timeline	Date Completed	Notes
Evaluation				
8. Evaluation				
Collect feedback forms from exercise participants.	[Evaluators]	[Immediately following exercise]		
Data Analysis Meeting Evaluator(s) and the scribe will consolidate data collected during and after the exercise to identify strengths, challenges, and other observations to determine if the exercise objectives were met. These findings will influence the AAR/IP.	[Lead Evaluator, Evaluators, Scribe]	[1 week after exercise]		
Distribute draft AAR/IP to participating organizations' for initial review	[Resource/ Logistics Lead]	[1 month after exercise]		
After Action Meeting				
Improvement Planning				
9. Improvement Planning				
Draft After Action Report / Improvement Plan (AAR/IP)	[Lead Evaluator]	[1 month after exercise]		
Distribute draft AAR/IP to participating organizations' for initial review	[Resource/ Logistics Lead]	[1 month after exercise]		

Exercise Planning Tasks	Assigned To	Suggested Timeline	Date Completed	Notes
After Action Meeting AAM's are typically used to review the AAR/IP and finalize findings. During the AAM meeting, discussions could take place on exercise results, observations, and identified areas of improvement such as corrective actions. By the end of the meeting, the Exercise Leadership Team may try to reach a consensus among the participants on exercise strengths and draft corrective actions.	[Exercise Leadership Team]	[1 month after exercise]		
Finalize AAR/IP	[Exercise Leadership Team]	[2 weeks after AAM]		
Recruit Commissioners or PUC leadership to champion the lessons learned, best practices, and successes identified in AAR/IP.	[Exercise Leadership Team]	Ongoing		
Track AAR/IP implementation and progress.	[Commissioners, PUC Leadership, or Exercise Leadership Team]	Ongoing		

Appendix C. Template Situation Manual

(SitMan - including Agenda and Feedback Form)



[Exercise Name]

Situation Manual

[Date]

This Situation Manual provides the run-of-show for a Cybersecurity Tabletop Exercise (TTX) conducted by **[Commission Name]** on **[Date of Exercise]** with **[List Other Participants]**. This document describes the exercise's background and purpose, as well as the functional aspects of the exercise. Due to the sensitive nature of the topics being discussed, this manual is designated as For Official Use Only (FOUO), and may not be distributed without written permission from [Name].

Royalty Free Photo Sources:

https://pixabay.com/illustrations/hacking-cybercrime-cybersecurity-3112539/
https://pixabay.com/illustrations/password-security-password-security-4993196/
https://pixabay.com/illustrations/phishing-fraud-cyber-security-3390518/
https://www.pexels.com/photo/blaze-blue-blur-bright-266896/
https://pixabay.com/illustrations/security-internet-crime-cyber-4700820/
https://unsplash.com/photos/WkfDrhxDMC8

Preface

The *[Exercise Name]* exercise is sponsored by the *[Commission Name]*. This Situation Manual (SitMan) was produced with input, advice, and assistance from the [Exercise Name] Planning Team, which followed the guidance set forth by the National Association of Regulatory Utility Commissions' (NARUC) Cybersecurity Tabletop Exercise Guide.

The *[Exercise Name]* Situation Manual (SitMan) provides exercise participants with all the necessary tools for their role(s) in the exercise and is evidence of *[Commission Name]*'s commitment to protecting the State of [State] and critical infrastructure sectors from cyber-attacks.

[Exercise Name] is an unclassified but *For Official Use Only (FOUO)* exercise. Sensitive topics may be discussed that are not permitted to be disclosed publicly under *[reference authority]*. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

Handling Instructions

1. The title of this document is the "*[Exercise Name]* Tabletop Exercise (TTX) Situation Manual (SitMan)."
2. Information gathered in this SitMan is designated as *For Official Use Only (FOUO)* and should be handled as sensitive information that is not to be disclosed. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. **Reproduction of this document, in whole or in part, without prior approval from [Commission Name] is prohibited.**
3. At a minimum, the attached materials will be disseminated strictly on a need-to-know basis and, when unattended, will be stored in a locked container or area that offers sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.
4. For more information about the exercise, please consult the following points of contact (POCs):

Exercise Director:
[Name]
[Title]
[Organization]
[Email Address]

Exercise Leadership Team:

[Name]	[Name]	[Name]
[Title]	[Title]	[Title]
[Organization]	[Organization]	[Organization]
[Email Address]	[Email Address]	[Email Address]

Safety Instructions

For this exercise, the below bullets define the protocols for differentiating real-world emergencies and simulated exercise events.

In-Person TTX Exercise Protocols:

- If the exercise requires the transmittal of information via phone, exercise participants should begin the simulated conversations with *"Exercise, Exercise, Exercise"* to avoid confusion with real-world events.
- If the exercise requires the transmittal of information via email or other written communications, *"Exercise, Exercise, Exercise"* should appear at the top of the message to avoid confusion with real-world events.
- When communicating with other exercise participants in-person, you are free to immerse yourself in the simulated events without regularly defining that they are partaking in an exercise. If information needs to be shared about a real-world emergency, participants should preface the information by saying *"time out from the exercise"* and use their hands to create a capital "T". To resume exercise play after the real-world emergency information was addressed, you can say *"resuming exercise."* This will avoid confusion among exercise participants about what is real and what is simulated.

Virtual TTX Exercise Protocols:

- [Depending on the features included with the virtual meeting platform and/or conferencing system, include safety protocols here. They should closely resemble the In-Person protocols above for consistency.]

Table of Contents

Agenda – [Exercise Name]

[Date]

8:30 – 9:00 am	Registration
9:00 – 9:05	Welcome – [Name]
9:05 – 9:20	Exercise Introduction and Overview – [Exercise Facilitator(s) Name(s)]
9:20 – 9:25	Inject 1 – [Inject 1 Name]
9:25 – 9:30	Functional Group Discussion[23]
9:30 – 9:55	Entire Group Discussion Period[24]
9:55 – 10:10	Brief Out[25]
10:10 – 10:15	Inject 2 - [Inject 2 Name]
10:15 – 10:20	Functional Group Discussion
10:20 – 10:45	Entire Group Discussion Period
10:45 – 11:00	Brief Out
11:00 – 11:05	Inject 3 - [Inject 3 Name]
11:05 – 11:10	Functional Group Discussion
11:10 – 11:35	Entire Group Discussion Period
11:35 – 11:50	Brief Out
11:50 – 12:30	Hot Wash[26] - [Exercise Facilitator(s) Name(s)]
12:30 pm	Lunch and networking

23 Function Group Discussion: Intra-organization discussion based on the inject.

24 Entire Group Discussion Period: Inter-organization discussion based on the inject and Functional Group Discussion.

25 Brief Out: Exercise facilitator(s) will lead an overview of the discussion and describe the mock actions that took place throughout the discussion period.

26 Hot Wash: Immediately following completion of the exercise, the Exercise Team can hold a "Hot Wash". A Hot Wash allows participants to provide feedback on how they thought the exercise progressed and how they themselves performed. Exercise strengths and areas that may need improvement are usually also discussed during this portion of the exercise.

Introduction

Background

The *[Commission Name]* works closely with electricity and natural gas utilities within the State of [State] in a regulatory and operational matter. After recent discussions with [Utility(s)] about cybersecurity strategies and posture, the *[Commission Name]* and *[Utility(s)]* decided to execute a cybersecurity focused tabletop exercise (TTX) to identify capabilities and practice response and recovery actions.

Purpose

The purpose of this exercise is to provide state officials and private sector utility representatives an opportunity to evaluate *[State]*'s emergency energy response protocols as they relate to any cybersecurity incident of significance. Among other things, this exercise will test protocols outlined within our state's *[Energy Assurance Plan / State Emergency Operations Plan]* and *[Cyber Annex]*.

[Additional/Targeted Purpose]

Exercise Objectives

[An objective should be specific, measurable, achievable, relevant, and time-bound (SMART)[27].]

[E.G. Following a cyber incident on energy infrastructure, review the ability of the PUC to utilize state, regional, and national communication networks in a timely manner to coordinate unity of effort and unity of message.]

Participants

- **Players.** Based on their organizational role and knowledge of current plans and procedures, players respond to the situation presented in the same way they would respond in reality.
- **Observers.** Observers primarily observe the exercise for their edification but may participate as much as the exercise facilitator(s) allows and/or they see fit.
- **Facilitators.** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the TTX.

Exercise Structure

The *[Exercise Name]* tabletop exercise (TTX) will be a group discussion based and mediator facilitated exercise. Players will participate in the following three injects:

- Inject 1: *[Inject 1 Name]*
- Inject 2: *[Inject 2 Name]*
- Inject 3: *[Inject 3 Name]*

After these functional group discussions, participants will engage in a facilitated group discussion in which a spokesperson from each functional group will present a synopsis of the group's actions, based on the scenario. From here, the entire group will discuss how each organization's actions impact one another and what type of coordination may need to take place.

Exercise Guidelines

- This is an open, low-stress, no-fault environment. The discussions will explore the policies, decisions, actions, and key relevant issues, which will require participants to respect the observations, opinions, and perspectives of others.
- Treat the scenario incidents as real. (i.e., don't fight the exercise)

27 https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

- Respond based on your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from training.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response and preparedness efforts. Problem-solving efforts should be the focus.
- Keep the time constraints in mind and comments focused, where possible.

Exercise Assumptions

In any exercise, several assumptions and artificialities may be necessary to complete play in the time allotted. During this exercise, the following apply:

- The scenario is plausible, and events occur as they are presented.
- There is no "hidden agenda", nor any trick questions.
- All players receive information at the same time.
- When possible, discussions and decision-making should be informed, first, by active plans, policies, and procedures outlined in the *[Energy Assurance Plan or State Emergency Operations Plan and/or Cyber Annex]*. If this presents an obstacle for the group as it progresses through the inject, discussions and decision-making can be hypothetical and based on group consensus when possible.

Inject 1: [Inject 1 Name]

[Date/Time of Inject]

[Insert Inject 1 here]

Key Issues

- [e.g., the IT Director is on vacation and unreachable]
- [Insert other key issues]

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Inject 1. Identify any additional requirements, critical issues, decisions, or questions that should be addressed at this time.

The following questions are provided as suggested general subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- [e.g., who should be a contacted first in this scenario]
- [other questions to encourage discussion]

Inject 2: [Inject 2 Name]

[Date/Time of Inject]

[Insert Inject 2 here]

Key Issues

- [e.g., the IT Director is on vacation and unreachable]
- [Insert other key issues]

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Inject 2. Identify any additional requirements, critical issues, decisions, or questions that should be addressed at this time.

The following questions are provided as suggested general subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- [e.g., who should be a contacted first in this scenario]
- [other questions to encourage discussion]

Inject 3: [Inject 3 Name]

[Date/Time of Inject]

[Insert Inject 3 here]

Key Issues

- [e.g., the IT Director is on vacation and unreachable]
- [Insert other key issues]

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Inject 3. Identify any additional requirements, critical issues, decisions, or questions that should be addressed at this time.

The following questions are provided as suggested general subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- [e.g., who should be a contacted first in this scenario]
- [other questions to encourage discussion]

Participant Feedback Form

Please enter your responses in the form field or checkbox after the appropriate selection.

Participant Name:_____ Title:_____ Agency:_____

Role (please place a checkmark in one of the boxes below):

☐ Player ☐ Observer ☐ Facilitator ☐ Evaluator

Part I – Recommendations and Action Steps

Based on discussions today and the tasks identified, list the top 3 issues and/or areas that need improvement.

_____

_____

_____

_____

Identify the action steps that should be taken to address the issues identified above. For each action step, indicate if it is a high, medium, or low priority.

_____

_____

_____

_____

Describe the action steps that should be taken in your area of responsibility. Who should be assigned responsibility for each action item?

_____

_____

_____

_____

List the policies, plans, and procedures that should be reviewed, revised, or developed. Indicate the priority level for each.

_____

_____

_____

_____

Is there anything you saw in the exercise that the evaluator(s) might not have been able to experience, observe, and/or record?

_____

_____

_____

_____

Part II – Exercise Design and Conduct

What is your assessment of today's exercise?
Please rate, on a scale of 1 to 5, the assessment factors listed below, with 1 indicating strong disagreement with the statement and 5 indicating strong agreement.

a.	The exercise was well structured.	1	2	3	4	5
b.	The exercise scenario was plausible and realistic.	1	2	3	4	5
c.	The Situation Manual was useful.	1	2	3	4	5
d.	This exercise would be useful for someone in my position.	1	2	3	4	5
e.	The participants included the right people at the right appropriate level.	1	2	3	4	5

What changes would you make to improve this exercise?
Please provide any recommendations on how this and future exercises could be more useful to you.

_____

_____

_____

_____

What additional training or experience would you like to have?

_____

_____

_____

_____

Appendix D. Template Exercise Evaluation Guide (EEG)

[Commission Name]:	Name of Exercise:
Location:	Date:
Evaluator:	Evaluator Contact Info:

Objective 1: [Name of Objective]	
Objective: [e.g., Following notification of a cyber incident affecting energy infrastructure with physical consequences, identify applicable capabilities, and associated authorities, the PUC can employ in response.]	
Observations of Capabilities that Address the Objective (can be positive or negative):	**Time of Observation**
1. [e.g., Jane, XYZ Commission staffer, discovered that a malicious cyber actor had gained control of XYZ Utility's SCADA system, then convened ESF #12 responders within the state to brief on the situation] [e.g., John Doe, a Cyber Analyst for XYZ Utility, discovered a cybersecurity breach, then texted his boss about it. His boss responded right away and informed the state's emergency management agency (EMA). The EMA immediately informed the PUC as the ESF #12 lead.]	[e.g., immediately after the PUC became aware of the incident] [e.g., 10:00 AM, one hour after the discovery of the incident]
2.	
3.	

Objective 2: [Name of Objective]	
Objective:	
Observations of Capabilities that Address the Objective (can be positive or negative):	**Time of Observation**
1.	
2.	
3.	

Objective 3: [Name of Objective]	
Objective:	
Observations of Capabilities that Address the Objective (can be positive or negative):	**Time of Observation**
1.	
2.	
3.	

Hot Wash Discussion Notes: The purpose of this section is to provide a space for evaluators to note important discussions during the Hot Wash that immediately follows the exercise. A Hot Wash allows participants to give feedback on how they thought the exercise progressed and how they performed. Exercise strengths and areas of improvement also discussed during this session. The Hot Wash may be led by the Lead Facilitator, who ensures that discussion points remain on topic and relevant to the objectives and goals laid out by the commission at the beginning of the exercise. Evaluators may use the information collected from the Hot Wash to draft an After Action Report/Improvement Plan (AAR/IP).

List the top three (3) organizational strengths:
1.
2.
3.

List the top three (3) items requiring improvement:
1.
2.
3.

Exercise Evaluation Guide Analysis Sheets: The purpose of this section is to provide a narrative of what was observed by the evaluator(s) for inclusion in the After Action Report/Improvement Plan (AAR/IP). This section includes a chronological summary of what occurred during the exercise. This section also suggests that the evaluator describe key observations (strengths or areas for improvement) to provide feedback to the exercise participants and support the sharing of lessons learned.

[i.e., Write a general chronological narrative of responder actions based on evaluator(s) observations during the exercise. Provide an overview of observations and, specifically, discuss how particular capabilities were carried out during the exercise, referencing specific tasks where applicable. The narrative provided will influence the After-Action Report/Improvement Plan (AAR/IP). If appropriate, make recommendations for improvement for each observation.

[Insert text electronically or on separate pages]

Appendix E. Template After Action Report/Improvement Plan (AAR/IP)



[Exercise Name]

After Action Report/Improvement Plan

[Date]

This After-Action Report/Improvement Plan (AAR/IP) is based on a Cybersecurity Tabletop Exercise (TTX) conducted by *[Commission Name]* on *[Date of Exercise]* with [List Other Participants]. This report provides an overview of the goals/objectives of the exercise, describes the scenario used to test capabilities, and suggests corrective actions to improve *[Insert Based on Objectives]*. Due to the sensitive nature of the topics being discussed, this report is designated as For Official Use Only (FOUO), and may not be distributed without written permission from *[Name]*.

Royalty Free Photo Sources:
https://pixabay.com/illustrations/cyber-security-protection-technology-3411476/
https://unsplash.com/photos/iIJrUoeRoCQ
https://unsplash.com/photos/fmTde1Fe23A

Exercise Overview

Name	[Exercise Name]
Date / Location	[Date] / [Location]
Scope	[i.e., Description of exercise type (Cyber TTX), participation level, exercise location, exercise duration, etc.]
Scenario	[Brief description of the exercise scenario]
Objective(s)	[Objective 1] [Objective 2] [Objective 3]
Sponsor	[Commission Name]
Participants	[Participating Organizations]

Exercise Summary

[Chronological summary of the exercise, including a full summary of the exercise scenario and injects]

[Description of key findings based on the exercise (i.e., What worked? What didn't work? Why or why not?)]

Objective	Performed without Challenges (P)	Performed with Some Challenges (S)	Performed with Major Challenges (M)	Unable to be Performed (U)
[Objective 1]				
[Objective 2]				
[Objective 3]				

Performed without Challenges (P): The targets and critical tasks associated with the preparedness capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. The performance of this activity did not contribute to additional health and/or safety risks for the public or emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

Performed with Some Challenges (S): The targets and critical tasks associated with the preparedness capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. The performance of this activity did not contribute to additional health and/or safety risks for the public or emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws. However, opportunities to enhance effectiveness and/or efficiency were identified.

Performed with Major Challenges (M): The targets and critical tasks associated with the preparedness capability were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or emergency workers; and/or was not conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

Unable to be Performed (U): The targets and critical tasks associated with the preparedness capability were not performed in a manner that achieved the objective(s).

Objective 1 Summary

Objective 1

[Objective Description]

Strengths:

- [List strengths]

Areas for Improvement:

- [List areas for improvement]

Objective 2 Summary

Objective 2

[Objective Description]

Strengths:

- [List strengths]

Areas for Improvement:

- [List areas for improvement]

Objective 3 Summary

Objective 3

[Objective Description]

Strengths:

- [List strengths]

Areas for Improvement:

- [List areas for improvement]

Improvement Plan

Issue/Area for Improvement	Corrective Action	Capability Element[28]	Recommended Responsible Organization	Target Completion Date
Objective 1: [Objective Description]				
[e.g., While following the EAP, it was unclear which agency was responsible for coordinating with DOE/FBI/DHS during a cyber incident.]	[e.g., Energy assurance plans should provide more detailed plans and approaches for dealing with cyber incidents, and should include the roles and responsibilities of all the state agencies that could be involved in the responses and public messaging. States should be prepared to identify what planning, policy, and regulatory actions have already taken place, and align them with Presidential Policy Directive (PPD)-41.]	[e.g., Planning /Organization]		
Objective 2: [Objective Description]				
Objective 3: [Objective Description]				

28 Capability Elements are: Planning, Organization, Equipment, Training, or Exercise.

List of Participants

Name	Organization	Email

Appendix F. Other TTX Guide Resources

Homeland Security Exercise and Evaluation Program (HSEEP)[29]

The HSEEP is a detailed overview of how to design, conduct, and evaluate an exercise. The document provides a set of fundamental principles for exercise programs, as well as a common approach to program management, design and development, conduct, evaluation, and improvement planning. If designing an advanced exercise, the HSEEP is a useful resource.

Emergency Planning Exercises[30]

FEMA has created a collection of templates on how to design a TTX for various types of emergency scenarios (including a cyber emergency). The collection of templates includes presentations, exercise facilitator notes, and video injects for multiple scenarios.

DHS Cybersecurity Services Catalog for SLTT Governments[31]

This catalog lists and describes cybersecurity services available to the SLTT community. The purpose of the catalog is to inform the SLTT community of these services (including exercise support), advance information sharing among the community, and promote the protection of SLTT systems. All services featured in this catalog are voluntary, non-binding, no cost, and available to stakeholders upon request.

Environmental Protection Agency (EPA) TTX Tool[32]

The EPA has developed a TTX tool for water and wastewater providers that is adaptable to any scenario.

COVID-19 Recovery CISA Tabletop Exercise Package (CTEP)[33]

The DHS's Cybersecurity and Infrastructure Security Agency (CISA) developed a COVID-19 Recovery CTEP to assist private sector stakeholders and critical infrastructure owners and operators in assessing short-term, intermediate, and long-term recovery and business continuity plans related to the COVID-19 pandemic.

---

29 HSEEP: https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

30 Emergency Planning Exercises: https://www.fema.gov/emergency-planning-exercises

31 DHS Cybersecurity Services Catalog for SLTT Governments: https://www.us-cert.gov/sites/default/files/c3vp/sltt/SLTT_Hands_On_Support.pdf

32 https://www.epa.gov/waterresiliencetraining/develop-and-conduct-water-resilience-tabletop-exercise-water-utilities

33 COVID-19 Recovery CTEP: https://www.cisa.gov/publication/covid-19-recovery-ctep-documents

Appendix G. Other Support Resources and Considerations

State-Specific Support Sources:

- In most states, the Emergency Management Agency conducts an annual emergency response exercise. Consider requesting a cybersecurity scenario related to energy for an upcoming statewide exercise.
- Reach out to your state's Emergency Management Agency, State Administrative Agency, Governor's Office, or other agency as appropriate and inquire about available funding to conduct a TTX focused on cybersecurity. If funding is available, possibly federal funding through a specified state agency, it could be used to hire professional assistance, such as facilitators, evaluators, scribes, cybersecurity SMEs, or secure an off-site venue.

Federal Support Sources:

- The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) hosts a biennial cybersecurity exercise known as Liberty Eclipse, which is open to participation from PUCs. In addition to Liberty Eclipse, DOE CESER partners with other federal agencies on a variety of cybersecurity-related exercises. Reach out to DOE CESER by emailing exercises@hq.doe.gov to ask about upcoming cybersecurity exercises open to PUCs.
- The Federal Emergency Management Agency's (FEMA) Emergency Management Institute (EMI) conducts Virtual Tabletop Exercises (VTTX) using a video teleconference (VTC) platform to reach community-based training audiences around the country. The VTTX process involves key personnel from the emergency management community of practice reviewing a prepackaged set of exercise materials, then convening for a 4-hour TTX discussing a simulated disaster scenario with a total of 10 to 15 individual sites participating. The event allows the connected sites to assess current plans, policies, and procedures while learning from the other participants. A VTC system is required for participation; there is no cost for this program. Find additional information here: https://training.fema.gov/programs/emivttx.aspx.
- A source of financial support could come from the federal government in the form of Energy Emergency Preparation Grants (EMPG) or the Homeland Security Grant Program (HSGP). These grants may be used to conduct a cybersecurity exercise. Commission staff can check with their state governor's office to determine if they have access to these funds.
    - EMPGs are issued by FEMA and can be used to conduct a national security exercise. However, only state Emergency Management Agencies and State Administrative Agencies (SAA) can apply for these grants; a commission cannot directly apply.[34] Commission staff may wish to speak with their SAA or state emergency management agency to find out what funds are available and how they may access them.
    - The HSGP provides support to enhance the ability of state, local, tribal, and territorial (SLTT) governments, as well as nonprofits, to prevent, protect against, respond to, and recover from terrorist attacks. HSGP is composed of three grants programs, including the State Homeland Security Grant Program (SHSP), the Urban Area Security Initiative (UASI), and Operation Stonegarden (OPSG). State Administrative Agencies (SAA) are the only entities eligible to apply for HSGP grants.[35]

34 Emergency Management Performance Grant Program: https://www.fema.gov/emergency-management-performance-grant-program

35 Homeland Security Grant Program: https://www.fema.gov/homeland-security-grant-program | https://www.fema.gov/media-library-data/1581619107442-915cab1ee9d3eaece7aa50d6bc439c52/FY_2020_HSGP_Fact_Sheet_GPD_Approved_508AB.pdf

- The "SHSP assists state, tribal, and local governments with preparedness activities that address high-priority preparedness gaps across all preparedness core capabilities where a nexus to terrorism exist.
- UASI assists high-threat, high-density urban areas to build and sustain the capabilities necessary to prevent, protect against, mitigate, respond to, and recover from terrorist attacks.
- OPSG supports enhanced cooperation and coordination among Customs and Border Protection, U.S. Border Patrol, and local, tribal, territorial, state, and federal law enforcement agencies."[36]

- State emergency management agencies typically have 5-year exercise planning calendars and annual coordination meetings in conjunction with the HSGP activities. Commissions may consider contacting state emergency management about participating in that process and working with other agencies to develop a cyber TTX.
- Commissions may also consider working with their Department of Homeland Security (DHS) regional Protective Security Advisors on accessing any available federal support for a cyber exercise.

Utilities and/or Other Private Entities:

- Reach out to utilities and other entities and inquire about any cybersecurity exercises they may already have planned. If they already plan on conducting one, they may be open to PUC participation.
- Open to PUCs and conducted biennially, GridEx is a grid security exercise series sponsored by the North American Electric Reliability Corporation's Electricity Information Sharing and Analysis Center.[37] The GridEx exercise series focuses on cyber and physical disruptions to the bulk power system. Commissions should contact stakeholders within their state and inquire about collaboratively participating in future GridEx exercises.

36 Department of Homeland Security Preparedness Grants: A Summary and Issues, p. 5–6: https://fas.org/sgp/crs/homesec/R44669.pdf

37 GridEx: https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEx.aspx

NARUC
National Association of Regulatory Utility Commissioners

1101 Vermont Ave, NW • Suite 200 • Washington, DC 20005
www.naruc.org • (202) 898-2200