Supplemental Project Notice

CYBER SECURITY INCIDENT RESPONSE AND RECOVERY TABLETOP EXERCISE

PROJECT HIGHLIGHTS

- Tests Utility Incident Response and Recovery plans in a workshop environment that is facilitated by EPRI as an independent party
- Complete NERC CIP compliance requirement
- Identifies and documents ways the utility can improve internal processes and procedures
- Validates roles, responsibilities, and authorities involved in cyber incident.

Background, Objectives, and New Learnings

It is critical for utilities to continually evaluate and exercise their capabilities to effectively respond to cyber security events in their operational environments to determine if their processes satisfy detection, response, and recovery requirements. With the increased inclusion of and dependence on processor-based power delivery and communications infrastructure, the potential for attacks by malevolent cyber agents also increases. NERC CIP-008 and CIP-009 require utilities to test their Incident Response and Recovery plans.

A tabletop exercise (TTX) is a facilitated, scenario-based workshop that tests an organization's ability to respond to scenarios in a practice environment. It enables participants to review and discuss in detail the actions they would take to validate operational processes, procedures, roles, responsibilities, and reporting structures. The key outputs of the TTX are an identification of people, process, and technology gaps and recommendations to resolve them.

Benefits

This project provides the ability for the funding utilities to exercise their Incident Response and Recovery plans in a workshop environment that is facilitated by EPRI as an independent party. The exercise or test of the plan is a requirement of the North American Electric Reliability Corporation critical infrastructure protection regulations CIP-008 and CIP-009. In addition, in support for the utility's regulatory compliance, the project will identify ways the utility can refine the processes and procedures that personnel in different roles within the organization must follow in a cyber event.

The project will also aid the utility in validating the roles, responsibilities, and authorities involved in cyber incident response and recovery , including documenting the following answers:

- Who is the primary authority to orchestrate action in the response and recovery phases?
- Who performs cyber-related analysis of the operational environment?
- Who are the stakeholders?

- How is information shared?
- How is mandatory reporting accomplished?

Observations by the facilitation team about technology/process/skills gaps and mitigation recommendations will be included in the report deliverable.

Project Approach and Summary

A kickoff meeting will be held with each utility to determine attendee requirements, meeting logistics including date and location, and use cases for the actual tabletop exercise. The project will utilize the process illustrated below to conduct the tabletop exercise and document the results:

The tabletop exercise participants will be made up of three teams:

1. White Team – facilitation
2. Red Team – attacker or adversary
3. Blue Team – responder

The results of the exercise will be delivered as an EPRI report and will include an appendix that will serve as evidence for NERC compliance.

Deliverables

- Preparation meeting with member to define:
  - Use cases for the exercise
  - Required utility attendees
  - Utility documentation required for the workshop, such as the network architecture for the environments to be covered by the use cases, and the Incident Response and Recovery Plan
- Conduct the tabletop exercise as a one-day workshop at the utility's selected location
- A written report that summarizes the observations, gaps, recommendations for Incident Response and Recovery plan improvements, and a section that satisfies NERC CIP reporting requirements for the utility

Price of Project

Each tabletop exercise is designed for a specific utility and is independent of other members.

The cost is $67.5k per utility.

The project qualifies for self-directed funding (SDF) or Co-funding.

Project Status and Schedule

The duration for each member engagement will be approximately 90 days. This includes the planning meeting, the workshop, and the report preparation and review.

Who Should Join

This project is applicable to all EPRI members responsible for cyber security incident response and recovery.

Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

Technical Contact

Chuck Moran at 650.855.8521, cmoran@epri.com

Technical Advisor Contact Information

West: Brian Dupin at 650.906.2936
bdupin@epri.com

Northeast: Barry Batson at 704.595.2873
bbatson@epri.com

Southeast: Annie Haas at 650.855.1031
ahaas@epri.com

Canada: Warren Frost at 403.474.4432
wfrost@epri.com

Product ID: 3002017679 **Project ID:** 01-107152 **February 2026**

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com
© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ENERGY are registered marks of the Electric Power Research Institute, Inc. in the U.S. and worldwide.