Supplemental Project Notice

CYBER SECURITY PROGRAM ASSESSMENT FOR UTILITY TRANSMISSION

PROJECT HIGHLIGHTS

- Gain actionable information and insights to improve OT cyber security posture and attack readiness
- Enact cyber security objectives and project plans based on utility-specific recommendations
- Access to EPRI's metrics portal to benchmark important utility cyber security readiness parameters and inform risk reduction priorities

Background, Objectives, and New Learnings

Utilities must objectively understand their cyber security posture and capabilities within their operation technology (OT) environments to develop the cyber security plans that help ensure continued grid reliability and resiliency.

Challenges in defining strengths and weaknesses are compounded by diverse SCADA options, legacy security offerings and multiple asset sites with different technologies and configurations.

Cyber security assessments typically report how well an existing system is prepared to manage its cyber security risks. These assessments provide baseline status reports and identify opportunities to improve OT cyber security.

This cyber security assessment project for power delivery systems does more than document observations about areas for improvement. The methodology produces recommendations for goals, plans, and timelines to enhance your OT cyber security operations. This project also collects data to create an overall readiness score that helps quantify utility OT preparations for a cyber attack.

Objective

The objective of this supplemental project is to deliver information and recommendations that address gaps and weaknesses in OT cyber security programs based on industry best practices and EPRI expertise. These assessments may:

- Aid utilities in prioritization of actions and development of project plan tasks and timelines aligned to results recommendations.
- Enhance collaborative research by aggregating anonymized assessment results so industry-wide trends, strengths and weaknesses, and best practices can be defined into readiness scores.
- Assist in building justifications for OT cyber security investments in technologies, practices, and workforce.

Benefits

Each assessment documents a cyber security baseline and identifies specific recommendations to improve cyber security posture and overall attack readiness for each participating utility. Objective recommendations may help utilities prioritize actions to mitigate risks. As each participant completes improvement goals identified in the assessment report, OT cyber risks may be mitigated. This project includes complimentary access to EPRI's Cyber Security Benchmarker for comparative, anonymized analysis of utility parameters.

Project Approach and Summary

Each Power Delivery Cyber Security Program Assessment will start with the basic assessment module. Additional assessment modules may be added based upon participant requirements. The assessment methodology may request specific data furnished by utilities and may include surveys and other tools to collect that data. The basic assessment module will be based on either the NIST Cybersecurity Framework (CSF) assessment or the Cybersecurity Capability Maturity Model (C2M2) assessment.

An assessment may include the following programmatic and performance areas as optional modules:

- Engineering design process
- Patch management and testing
- Transient cyber asset program
- Wireless access
- Remote access
- Tamper indication program
- Internal assessment and audit process
- Cyber security training

Deliverables

Each participating utility will receive:

- Confidential assessment report that documents observations, strengths, weaknesses, and prioritized opportunities for improvement based on EPRI expertise and relevant research.
- Action plan recommendations that identify the major milestones to inform project plans.
- Collaborative results report that aggregates and anonymizes research results from other assessments in EPRI's Cyber Security Benchmarker for a holistic view of the electricity subsector's overall OT cyber security attack readiness.
- Access to the EPRI Cyber Security Benchmarker to submit data and produce benchmark reports based on anonymized data. This complimentary access will expire two years after the completion of the funder's initial assessment report.

Price of Project

The basic assessment module using either the NIST CSF or C2M2 approach is priced at $85,000 per utility. Optional modules are priced at $7,500 per module. There is no minimum or maximum number of optional modules that can be selected for any utility assessment. This supplemental project qualifies for Self- Directed Funding (SDF) and Co-funding.

Project Status and Schedule

The project schedule is based on the assessment scope and availability of the participant's resources and facilities. A typical assessment may comprise two months from start to finish based on the scope. A schedule will be proposed and mutually agreed upon by each project participant and EPRI.

Who Should Join

Utilities seeking to leverage EPRI's expertise for objective evaluations of their OT cyber security programs should join this project. Utilities interested in benchmarking their results against other anonymized results to gauge OT cyber security program parameters should join this project.

Contact Information

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

Technical Contact

Esther Amullen, 650.855.1027 (eamullen@epri.com)

To Join, Contact Your Information, Communication, and Cyber Security Technical Advisor

West: Brian Dupin at bdupin@epri.com

Northeast: Barry Batson at bbatson@epri.com

Southeast: Chuck Wentzel at cwentzel@epri.com

Product ID: 3002020210 **Project ID:** 01-107152 **April 2025**

EPRI

3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com