EPRI

2024

AT A GLANCE

Cyber Security for Energy Delivery and Customer Solutions (ED&CS)

Program 183

Research Value

- **Enhanced Resilience Against Cyber Threats** – Develops and implements strategies for advanced cyber security measures.
- **Multidisciplinary Approach to Emerging Challenges** – Addresses the rapidly evolving cyber security threats to interconnected electric sectors with collaborative and multidisciplinary research.
- **Expert Insight and Analysis** – Leverages a team of cyber security experts who offer in-depth insights and analyses on security tools, architectures, and guidelines.
- **Proactive and Comprehensive Cyber Security Strategies** – Identify, address, and adapt to both current and future cyber security challenges, developing roadmaps and strategies to safeguard critical infrastructure.

Member Benefits

- **Access to Cutting-edge Research** – Gain exclusive access to the latest cyber security technologies and research findings to proactively safeguard infrastructure.
- **Expert Guidance and Support** – Benefit from direct support and insights from top cyber security experts, enhancing the ability to respond to and manage threats.
- **Collaborative Network Opportunities** – Engage with industry peers, sharing best practices and learning from collective experiences in cyber security challenges.
- **Tailored Cyber Security Strategies** – Receive customized advice and strategies for specific infrastructure needs, ensuring robust and effective cyber security measures are in place.

The Cyber Security for Energy Delivery and Customer Solutions program is a comprehensive initiative designed to fortify the electric grid against cyber threats.

Focusing on electric utilities, the program incorporates multidisciplinary research and expert collaboration to develop and implement advanced cyber security measures.

Members benefit from access to pioneering research, expert guidance, collaborative networks, and tailored strategies to address evolving cyber threats, ensuring the reliability and security of their infrastructure against a backdrop of rapid technological change.

The Cyber Security for ED&CS program focuses on the following issues:

- **Strategic Intelligence and Emerging Issues:** Focused on providing insights and guidance on strategic cyber security issues relevant to electric utilities.
- **Incident and Threat Management:** Develops comprehensive cyber security approaches encompassing incident management, threat analysis, and forensics.
- **Cyber Security for Transmission and Distribution:** Addresses specific challenges in digital substations and control centers, integrating cyber security into utility processes.
- **Cyber Security for DER and Grid Edge Systems:** Concentrates on risk management and secure integration of distributed energy resources (DER) with grid systems.
- **Cyber Security Data Applications:** Involves innovative data management strategies and the use of advanced analytics and AI for threat identification and mitigation.

Research Highlights

Strategic Intelligence & Emerging Issues (183A)

- **Guidance on Emerging Threats and Vulnerabilities:** Provides up-to-date intelligence and recommendations on newly emerging cyber security vulnerabilities, threats, and issues.
- **Dynamic Program Monitoring and Evolution:** Offers guidance for OT cybersecurity programs, alongside developing strategic roadmaps for adapting to emerging threats and technological advancements.

Incident Management & Threat Management (183B)

- **Comprehensive Incident and Threat Management:** Develops systems for monitoring, detection, and response to cyber security events, alongside procedures for managing and responding to threats.
- **In-depth ICS Forensics:** Focuses on conducting detailed forensic analysis of industrial control systems (ICS) devices.

Cyber Security for Transmission & Distribution (183C)

- **Targeted Security for Digital Substations and Control Centers:** Addresses unique cyber security challenges in digital substations and control centers.
- **Integrating Cyber Security into Utility Processes:** Focuses on integrating cyber security into utility planning, design, and operations, and developing best practices for long-term security standards in grid infrastructure.

Cyber Security for DER & Grid Edge Systems (183D)

- **Robust Cyber Security for DER Integration:** Develops comprehensive cyber security strategies, including risk narratives, frameworks, and engineering guidelines, to secure grid systems with distributed energy resources.
- **Practical Tools and Collaborative Efforts:** Creates practical engineering tools, reference architectures, and conducts field demonstrations, for resilient integration of DER.

Cyber Security Data Applications (183E)

- **Innovative Data Management and Analytics:** Develops advanced data management strategies and integrates machine learning for proactive cyber threat identification and mitigation.
- **Collaborative Cyber Security Advancements:** Focuses on collaborative efforts and continuous improvement in cyber security data applications, promoting industry-wide knowledge sharing.

EPRI Technical Contact
BEN SOOTER, *Program Manager*
865.218.8108, bsooter@epri.com

For more information, contact:

EPRI Customer Assistance Center
800.313.3774 • askepri@epri.com

3002028986 February 2024

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