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

Essence2.0 Development and Deployment

NRECA America's Electric Cooperatives

Strengthening a communitarian approach to securing electric utility infrastructures nationwide

Essence2.0 improves, refines, and deploys technology for detecting cyberattacks on utility supervisory control and data acquisition systems, operational technology, and information technology networks and assets. It also contains and remediates adversarial action. This project increases the testing and hardening of cybersecurity solutions developed during the Essence project, expands and diversifies deployments across electricity markets and utility types, and creates the organization and infrastructure needed to sustain operations and expand the cyber-defensive footprint at a national scale. It integrates and fuses two related technologies that enable energy delivery system operators to analyze both network behavior and the physics of electricity infrastructure in real time, operationalizing anomaly detection and autonomous defense across the energy sector. Essence shares information and tactics between participating utilities and has the capability to escalate to information sharing and analysis centers for further evaluation. External query capability functionality is also available. To maximize impact, Essence2.0 focuses on deploying solutions to smaller utilities that are not effectively addressed by the major commercial cybersecurity providers and who face financial barriers to implementing critical cybersecurity services.

KEY TAKEAWAYS

- Operationalizes anomaly detection and autonomous cyber-defense solutions across the energy sector
- Expands testing and hardening of operational and information technology security solutions developed during the previous Essence project
- Diversifies deployments and establishes communication structures required for community-supported cybersecurity at a national scale

OUTCOME

This project enables faster industry response to cyber and grid physical attacks by advancing the capabilities of the previous Essence anomaly detection engine. A wider footprint of coverage within the industry will be achieved through broader deployments of solutions and organizational structures to support community-driven security at utilities nationwide.

PARTICIPANTS	ROLE
NRECA America's Electric Cooperatives	Tests and improves technological advances through real-time coordinated responses with an organized community of nearly 900 member cooperatives. NRECA Research advances cyber and power grid awareness that address blended cyber and physical concerns with a focus on operational technology network impacts.
BLACKBYTE Cyber Security, LLC	Provides architectural designs to advance network and grid data collection techniques used in advanced analysis and visualizations.
referentia	Provides a high-performance data environment to advance analysis of network and grid metrics leveraged for total situational awareness and information sharing.

CONTACT INFORMATION

Initial Leads:

Doug Lambert
Principal Investigator
National Rural Electric Cooperative Association
571-420-1665
Doug.Lambert@nreca.coop

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: September 2020 – September 2023

Total Award Value: $7,435,043
DOE Share: $7,435,043
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021