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

CINDER: Cybersecure Integration of Networked Distributed Energy Resources

Lawrence Livermore National Laboratory

Applying CEDS technology at federal facilities

This pilot leverages cybersecurity control tools and technologies for energy management systems at U.S. Department of Defense (DoD) installations and U.S. Department of Veterans Affairs (VA) facilities. These tools and technologies include building automation, micro-grid and distributed energy resource (DER) integration and control, and smart metering and advanced sensing. They will be used to safely and reliably integrate patching and to provide continuous monitoring of these systems and other cybersecurity controls – strengthening the ability to survive a cyberattack. The Security Platform and Patch Management Program will be used to make recommendations on specific devices that can be implemented that have fewer vulnerabilities and will propose the optimal cybersecurity measures for the system. This pilot leverages Lawrence Livermore National Laboratory's network mapping tool (NeMS), CyberInterconnection Analysis Tool, and Safe Active Scanning for Energy Delivery Systems, and FoxGuard Solutions technology.

KEY TAKEAWAYS

- Informs the cyber risk strategy for future distributed energy resource and microgrid deployment
- Enhances the resilience of energy delivery systems by addressing potential threats introduced by highly dispersed controllable generation
- Combines two tools, a network mapping tool and a patch management tool, to make complex networks secure

OUTCOME

This project validates CEDS technologies in the operational environment to energy providers, supporting DoD and the VA, with a goal of bringing cybersecurity for energy delivery systems technology nationwide. The tools will transition to the DOD and the VA team members for integration into their risk management processes.

PARTICIPANTS	ROLE
Lawrence Livermore National Laboratory	Leverages the NeMS tool to scan demonstration partner networks and perform cyberattack scenario evaluations on digital twins of these networks
FoxGuard Solutions	Pilots the Security Platform and Patch Management Program with demonstration partners
VA | U.S. Department of Veterans Affairs	Initial pilot site; helps make the VA hospital's solar generation system more cybersecure with the combination of LLNL and FoxGuard Solutions tools
Hurlburt Field	Second pilot site; location where the Civil Engineer Community of Interest Network Enclave was scanned and digitally replicated for cyberattack scenario evaluation

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Emma Stewart
Principal Investigator
Lawrence Livermore National Laboratory
925-422-1902
stewart78@llnl.gov

Current Contact as of February 2020:

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: July 2018 – September 2020

Total Award Value: $2,000,000
DOE Share: $2,000,000
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