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

Department of Defense Installation Energy Resiliency Pilot Program

Pacific Northwest NATIONAL LABORATORY

Building strategic partnerships between the Department of Energy, Department of Defense, and the energy sector to provide awareness of software-defined networking capabilities in operational environments

The project team is advancing the Department of Defense's (DoD) ability to survive a cyberattack and validates cybersecurity for energy delivery systems (CEDS) technologies for energy providers supporting DoD installations by redesigning systems and network architecture and deploying tools and technologies from the CEDS R&D portfolio. The project uses operational technology (OT) software-defined networking (SDN) to secure multiple DoD OT systems. The project team has piloted OT-SDN technology on electric power infrastructure located at various locations. Each of the OT-SDN pilot demonstrations have utilized the same approach to ensure successful deployments. The team designed the pilot to capture lessons learned that will hasten the adoption of OT-SDN technology for multiple critical infrastructure systems by addressing barriers to technology adoption, building strategic relationships, identifying infrastructure resiliency requirements, and supporting the DoD Authority to Operate process. In addition to pilot tasks, cybersecurity, technology transition, and outreach are key focus areas of this project.

KEY TAKEAWAYS

- Improves the Department of Defense's energy system cybersecurity through strategic partnerships and coalition building
- Enhances the security and reliability of the nation's energy delivery infrastructure
- Uses operational technology software-defined networking technology to secure multiple types of energy delivery systems

OUTCOME

This project has developed a successful blueprint that can be used for future partnerships between the Department of Energy and the DoD. Lessons learned from each pilot location will be used to inform subsequent pilots. Integration of SDN technology into OT environments will make DoD cybersecurity best of class. U.S. Navy collaborators in Hawaii have described our effort as being a mission enabler. The Naval Facilities Engineering Command (NAVFAC) is proceeding with plans to expand the use of OT-SDN technology at 30 additional locations in the next two years. NAVFAC and Ft. Belvoir personnel are sponsoring the OT-SDN technology for the Defense Information Systems Agency Approved Product List.

PARTICIPANTS	ROLE
Pacific Northwest NATIONAL LABORATORY	Leads the OT-SDN pilot deployments that encompass DoD, Coast Guard, Veterans Affairs, and privatized electric utility service provider systems
NAVFAC Naval Facilities Engineering Command	Key sponsor for the deployment of OT-SDN across Navy installations and available on the Defense Information Systems Agency (DISA) Approved Products List.
SEL SCHWEITZER ENGINEERING LABORATORIES	Commercial vendor, training provider, and lead integrator for OT-SDN.
	Early adopter of OT-SDN technology with plans to expand both the size and types of critical infrastructure operating on an OT-SDN network; sponsor to make the OT-SDN technology available on the DISA Approved Products List.
SPECTRUM SOLUTIONS SSI	Integrator for the NVESD networks and a partner on other DOE and DoD SDN-focused projects; developed a situational awareness capability that integrates the health of both the critical infrastructure and OT-SDN network into a single solution.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Mark D. Hadley
Principal Investigator
Pacific Northwest National Laboratory
509-375-2298
mark.hadley@pnnl.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 – December 2021

Total Award Value: $4,000,000
DOE Share: $4,000,000
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