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

# Extended Cybersecurity Threat Information Sharing

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

*Sharing threat information from inside private networks by collecting and perturbing data to protect sensitive information*

This project develops an advanced cybersecurity threat information sharing solution for electric utilities to share threat intelligence that help prevent, detect, and respond to cyberattacks and improve the overall cybersecurity of the energy sector. The project team researches which data inside a utility's network should be shared as a type of cyber threat information. For those data that have value in threat information sharing but contain sensitive information, the team researches which data can be shared in a perturbed form and determines how to perturb these data. A low-cost, software sensing agent, which can run inside private networks and send the collected data to the analysis center, will be developed to collect the data.

## KEY TAKEAWAYS

- Shares threat intelligence securely collected from inside electric utilities' private networks
- Improves the quality of data shared between utilities by adding application-layer information
- Reduces costs related to installing expensive sensors by processing more information on customer-owned devices

## OUTCOME

This project identifies a set of data types to be shared from private utility networks and systems, develops a set of perturbation methods to protect sensitive information and alleviates utilities' concerns over data leakage, and develops a low-cost software sensing agent for collecting cybersecurity threat information and sharing with the analytics center.

| PARTICIPANTS | ROLE |
|---|---|
| SEEDS CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS | This project is part of the Secure Evolvable Energy Delivery Systems (SEEDS) academic consortium. SEEDS researches and develops innovative cybersecurity technologies, tools, and methodologies to advance the energy sector's ability to survive cyber incidents while sustaining critical functions. |
| UNIVERSITY OF ARKANSAS | Research, development, and testing |

## CONTACT INFORMATION


**Initial Leads:**

**Carol Hawk**
Program Manager

**Qinghua Li**
Associate Professor
University of Arkansas
479-575-6416
qinghual@uark.edu

**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



This is a subproject sponsored by the SEEDS academic consortium, led by the University of Arkansas.

**SEEDS Period of Performance:** October 2015 – March 2022

**SEEDS Total Award Value: $15,309,114**
DOE Share: $12,226,504
Cost Share: $3,082,610

**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