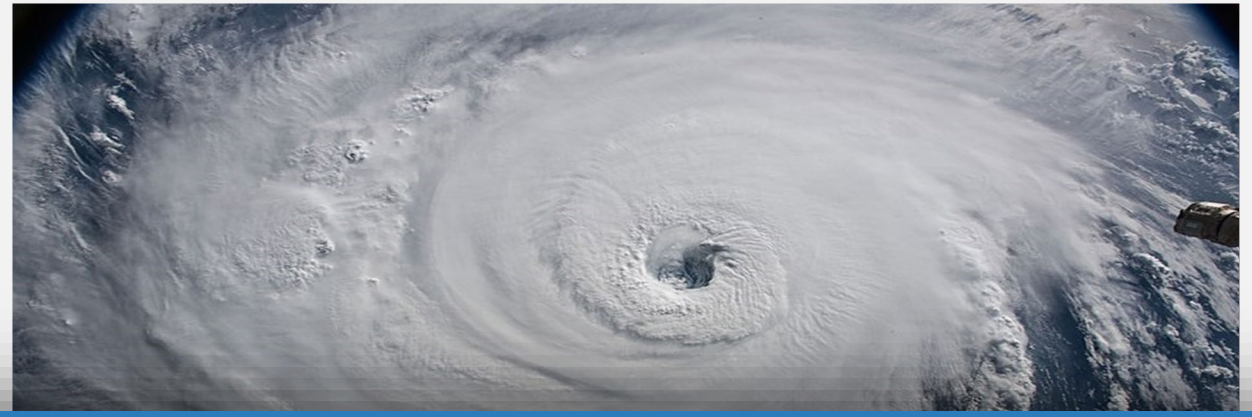


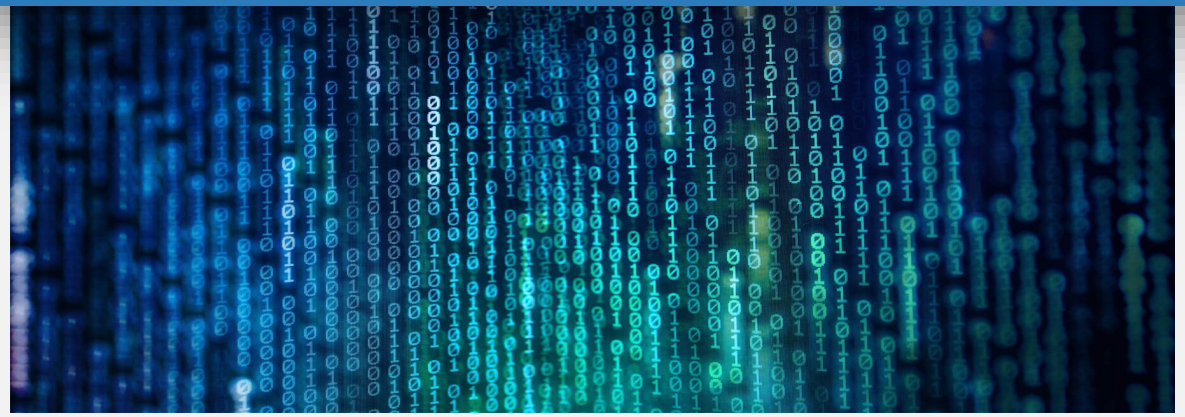
U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

8th Annual EPRI-IEA Workshop

Panel 3: Planning and Forecasting for Physical and Climate Resilience

Akhlesh Kaushiva, P.E., Senior Technical Systems and Cybersecurity Advisor, DOE CESER

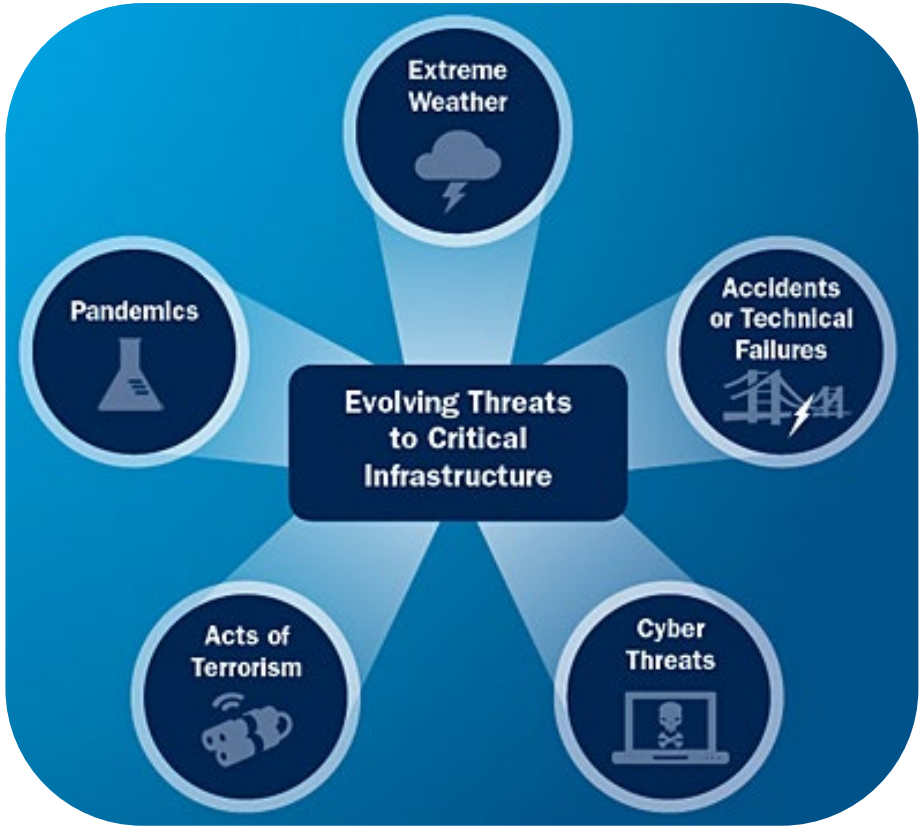
October 21, 2021



CESER Mission

To enhance the security of U.S. critical energy infrastructure to all hazards, mitigate the impacts of disruptive events and risk to the sector overall through preparedness and innovation, and respond to and facilitate recovery from energy disruptions in collaboration with:

- Energy owners and operators, manufacturers, and trade associations
- State, local, tribal, and territory governments
- Academia, National Labs, and the research community
- Energy information sharing and analysis centers (ISACs)
- Other Federal agencies (CISA, DOD, FBI)



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

Energy Security Threats and Trends

- Energy infrastructure and digital supply chain
- Energy systems are geographically dispersed and interdependent across multiple States, companies, and sectors, creating a multi-threat environment with the potential for cascading impacts during a disruption.
- Technological innovation and increasing connectivity are rapidly changing the risk posture for the energy sector.
- Energy sector companies are highly heterogenous; entities vary greatly in size, resourcing, and maturity level in capability to detect, deter, and mitigate cyber threats.
- The impacts of a changing climate and increasing natural hazards – such as wildfires and hurricanes – have affected millions of energy customers in the United States.

Cybersecurity for Energy Delivery Systems (CEDS) Division

- Accelerate the research, development and demonstration (RD&D) of next-generation cyber-resilient energy delivery systems and components.
- Identify triggering events and use cases which indicate anomalous activity on energy infrastructure.
- Make tools available for the energy sector companies to implement and enhance their on-site threat detection capability.
- Assist in improving the cybersecurity posture of sector entities using Cybersecurity Capability Maturity Model (C2M2) to strengthen their operational resilience.

Infrastructure Security & Energy Restoration (ISER) Division

- Preparedness & Incident Response and Recovery, and Training & Exercises.
- Develop a cyber vulnerability disclosure (CVD) program for operational technology in the energy sector through the Cyber Testing for Resilient Industrial Control Systems (CyTRICS™).
- Create actionable intelligence by linking threat information with supply chain information.
- Conduct state energy security planning and cyber threat information sharing for emergency response.

CESER Accomplishments & Initiatives

Clean Energy Cybersecurity Accelerator Program

- A new public-private partnership to advance cybersecurity measures for the Nation's evolving grid.

National Wind Cybersecurity Consortium

- Public-private consortium to identify use cases and develop a platform to improve intelligence on wind energy threats.

100-Day Industrial Control System (ICS) Plan

- A coordinated effort between DOE, the electricity industry, and the Cybersecurity and Infrastructure Security Agency (CISA).
- Confront cyber threats from adversaries with emphasis on OT.

America's Supply Chains Executive Order 14017 (February 24, 2021)

- Explores the full manufacturing supply chain, including raw materials, processed materials, subcomponents, final products, and end-of-life material recovery, as well as cybersecurity and software/digital infrastructure.

Ongoing R&D Efforts

National Rural Electric Cooperative Association:

Essence 2.0 Development and Deployment

Strengthening a communitarian approach to securing electric utilities infrastructures nationwide

- Previous DOE award developed technology relevant to OT cybersecurity
- Current effort is to install Essence 2.0 technology across ~30% of distribution coop sites
- Operationalize anomaly detection and autonomous cyber-defense

Lawrence Berkeley National Lab:

Supervisory Parameter Adjustment for Distribution Energy Storage (SPADES)

Automatic system reconfiguration to counteract cyberattacks

- Develop open-source methods and tools to protect energy storage systems
- Improve security and robustness of energy storage controls and connected devices

GE Global Research:

Cyber Physical Resilience for Wind Power Generation

Applies cyberattack detection and accommodation to wind farms

- Use physical models and machine learning to detect, localize, and accommodate for cyberattacks against wind turbines
- Provide scalable active defense against spoofing by physically watermarking communications

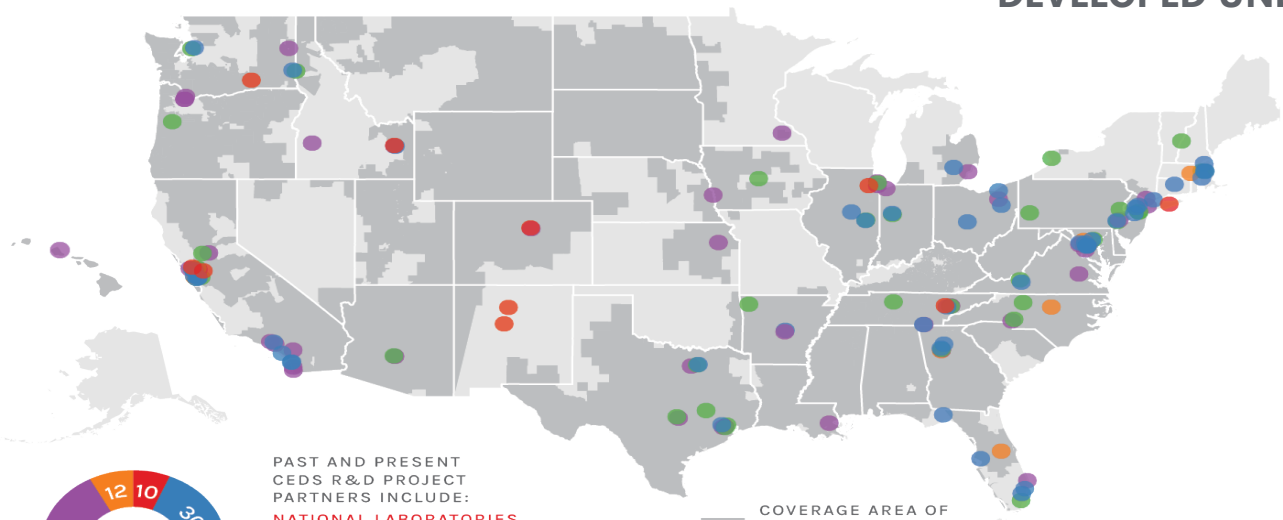
U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

CESER CEDS R&D: Reach and Impact

- **Funds earlier, high-risk/high-reward R&D** in areas critical for national security where a business case cannot readily be established by a private-sector company
- **Builds R&D pipeline through partnerships** with energy sector utilities, vendors and service providers, universities, and national laboratories

CEDS delivered **80 products**, tools, and technologies*
SINCE 2010 TO REDUCE ENERGY SECTOR CYBER RISK

More than **1,500** utilities in all **50** states
HAVE PURCHASED PRODUCTS DEVELOPED UNDER CEDS RESEARCH



57% of U.S. electricity customers are served by power providers participating in CEDS R&D

More than 155 partners have participated
IN COMPETITIVELY FUNDED PROJECTS

All CEDS projects included an **energy sector partner**
TO DRIVE REAL-WORLD SOLUTIONS

* As of December 2020

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

Contact Information

Akhlesh Kaushiva, P.E.
Senior Technical Systems and Cybersecurity Advisor
Cybersecurity for Energy Delivery Systems (CEDS)
Cybersecurity, Energy Security, and Emergency Response (CESER)
U.S. Department of Energy

akhlesh.kaushiva@hq.doe.gov

Office: 202-287-6062

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