U.S. DEPARTMENT OF
ENERGY

Office of
Electricity Delivery
& Energy Reliability

U.S. Department of Energy
Cybersecurity for Energy Delivery Systems (CEDS) Program
Research and Development (R&D)

Dr. Carol Hawk

March 28, 2017

U.S. Government Role and Responsibilities

Department of Homeland Security (DHS)

Provide strategic guidance, promote national unity of effort, and coordinate the overall Federal effort for secure and resilient critical infrastructure including identification and analysis of interdependencies among critical infrastructure sectors

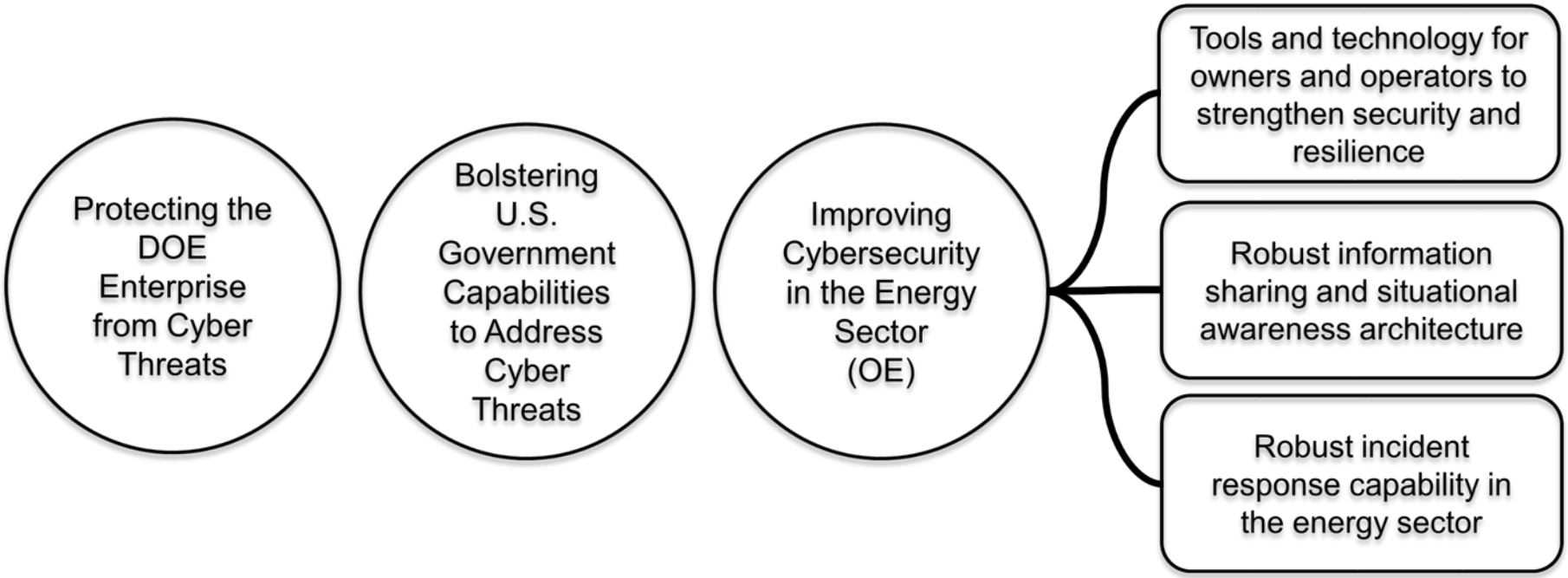
Critical Infrastructure Sector
• Chemical
• Commercial Facilities
• Communications
• Critical Manufacturing
• Dams
• Defense Industrial Base
• Emergency Services
• ***Energy***
• Financial Services
• Food and Agriculture
• Government Facilities
• Healthcare and Public Health
• Information Technology
• Nuclear Reactors, Materials, & Waste
• Transportation Systems
• Water and Wastewater Systems

DOE - Sector-Specific Agency (SSA) to:

- Collaborate with infrastructure owners and operators to strengthen the security and resilience of critical infrastructure
- Serve as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities
- Carryout incident management responsibilities consistent with statutory authority and other appropriate policies
- Provide technical assistance to the sector to identify vulnerabilities and help mitigate incidents

Department of Energy's Cybersecurity Roles

Office of Electricity Delivery & Energy Reliability (OE) focuses on DOE's role as a Sector Specific Agency (SSA)



Cybersecurity and Emerging Threats

Office of Electricity Delivery and Energy Reliability (OE)

CEDS R&D

Next-Generation Technologies

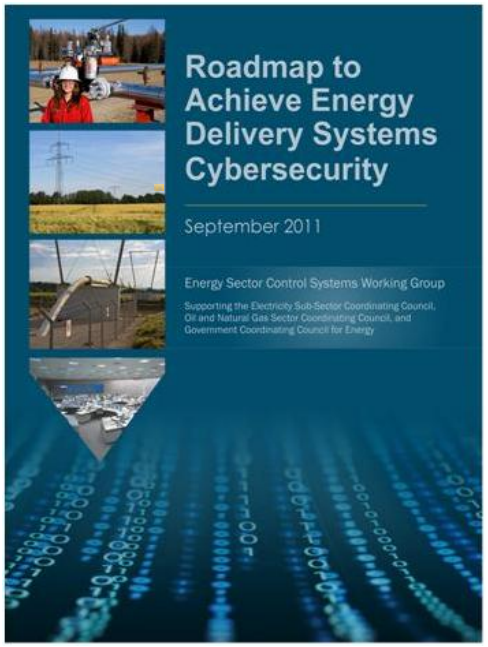
Research and develop tools and technologies to advance resilient energy delivery systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

CEDS OPS

Building Capabilities to Address Today's Threats

Make effective use of readily available existing technologies to create solutions to address immediate problems in the energy sector on a wide-scale basis through collaborations with industry.

Roadmap – Framework for Collaboration



- *Energy Sector's* synthesis of energy delivery systems security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in energy delivery systems security

Roadmap Vision

Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

Coordination with Other Federal Cybersecurity R&D Programs

- Primary mechanism for U.S. Government, unclassified Networking and IT R&D (NITRD) coordination
- Supports Networking and Information Technology policy making in the White House Office of Science and Technology Policy (OSTP)

CEDS Encourages Partnerships

Asset Owners/Operators

- Ameren
- Arkansas Electric Cooperatives Corporation
- Avista
- Burbank Water and Power
- BPA
- CenterPoint Energy
- Chevron
- ComEd
- Dominion
- Duke Energy
- Electric Reliability Council of Texas
- Entergy
- FP&L
- HECO
- Idaho Falls Power
- Inland Empire Energy
- NIPSCO
- Orange & Rockland Utility
- Pacific Gas & Electric
- Peak RC
- PJM Interconnection
- Rochester Public Utilities
- Sacramento Municipal Utilities District
- San Diego Gas and Electric
- Sempra
- Snohomish PUD
- Southern Company
- Southern California Edison
- TVA
- Virgin Islands Water and Power Authority
- WAPA
- WGES

Solution Providers

- ABB
- Alstom Grid
- Applied Communication Services
- Applied Control Solutions
- Cigital, Inc.
- Critical Intelligence
- Cybati
- Eaton
- Enernex
- EPRI
- Foxguard Solutions
- GE
- Grid Protection Alliance
- Grimm
- Honeywell
- ID Quantique
- Intel
- NexDefense
- OPAL-RT
- Open Information Security Foundation
- OSIsoft
- Parsons
- Power Standards Laboratory
- Qubitekk
- RTDS Technologies Inc.
- Schneider Electric
- SEL
- Siemens
- Telvent
- Utility Advisors
- Utility Integration Solutions
- UTRC
- Veracity
- ViaSat

Academia

- Arizona State University
- Carnegie Mellon University
- Dartmouth College
- Florida International University
- Georgia Institute of Technology
- Illinois Institute of Technology
- Iowa State University
- Lehigh University
- Massachusetts Institute of Technology
- Oregon State University
- Rutgers University
- Tennessee State University
- Texas A&M EES
- University of Arkansas
- University of Arkansas-Little Rock
- University of Buffalo - SUNY
- University of Illinois
- UC Davis
- UC Berkeley
- University of Houston
- University of Tennessee-Knoxville
- University of Texas at Austin
- Washington State

National Labs

- Argonne National Laboratory
- Brookhaven National Laboratory
- Idaho National Laboratory
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- National Renewable Energy Laboratory
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories

Other

- Energy Sector Control Systems Working Group
- International Society of Automation
- NESCOR
- NRECA
- Open Information Security Foundation

CEDS Research & Development Program Structure

Higher Risk, Longer Term Projects

- Core and Frontier National Laboratory Research Program
- Academia Projects

Medium Risk, Mid-term Projects

- National Laboratory Led Projects

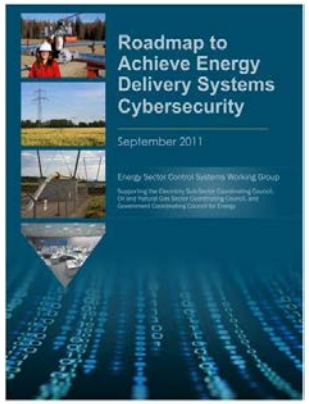
Lower Risk, Shorter Term Projects

- Energy Sector Led Projects

Partnering

Path to Transition to Practice in the Energy Sector

- CEDS builds research partnerships among energy sector utilities, asset owners and operators, suppliers, universities and national laboratories
- Successfully transitioned more than 30 tools and technologies that reduce the risk of energy delivery being disrupted due to a cyber incident in the energy sector
- Advancing the Roadmap's vision of *resilient energy delivery systems designed, installed, operated and maintained to survive a cyber incident while sustaining critical functions.*



Academic Collaboration Projects CREDC and SEEDS

ILLINOIS
UNIVERISTY OF ILLINOIS AT URBANA-CHAMPAIGN

Cyber Resilient Energy Delivery Consortium (CREDC)

- Published or presented research on:
  - Cost effective security management
  - Systematic and Systems theoretical approaches
  - Trustworthy critical infrastructure research
  - Tamper event detection using SCADA hardware
  - Detection of data injection attacks
  - Remote testbeds for experimenting in cyber-physical space

Partners

Old Dominion University 1930
Argonne NATIONAL LABORATORY
Massachusetts Institute of Technology
ASU Arizona State University
Oregon State University OSU
Tennessee State University
Rutgers University
Dartmouth
Pacific Northwest National Laboratory
University of Houston
Washington State University

UNIVERSITY OF ARKANSAS

Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)

- Project activities include:
  - Analysis, modeling, and detection of data and topology manipulation attacks, where grid connections are removed from system or their removal is spoofed
  - Visualization of real time data for situational awareness
  - Moving target defense, by frequently changing access information
  - Impact assessment of cyber attacks

Partners

UALR University of Arkansas at Little Rock
Massachusetts Institute of Technology
Lehigh University
Carnegie Mellon University
FIU Florida International University
Arkansas Electric Cooperative Corporation
We Are Arkansas

U.S. DEPARTMENT OF ENERGY | Office of Electricity Delivery & Energy Reliability

Opportunities to Engage with CREDC

Event	Description	Location	Date
Monthly CREDC Seminar Series	Presentation by Blake Larsen, CIO and Vice President of IT, Western Refining	Webinar	March 3, 2017
2017 CREDC Industry Workshop	Engage with CREDC researchers, learn about CREDC research activities, impact current and future research plans, and network with industry sector leaders.	Tempe, AZ	March 27-29, 2017
Monthly CREDC Seminar Series	Presentation by Michael M. Johnson, Chief Information Officer, U.S. Department of Energy (DOE)	Webinar	April 7, 2017
2017 CREDC Summer Training	Focus on cybersecurity and resiliency of energy delivery systems for the electric power and oil & gas industries	St. Charles, Illinois	June 11-17, 2017
Joint Information Trust Institute/CREDC and NRECA Cybersecurity Summit	Summit for electric cooperatives and municipal power providers	University of Illinois Champaign, IL	TBD
CREDC Industry Outreach Event	Industry-focused outreach event organized by PNNL, Washington State University, and Oregon State University	Pacific Northwest	November 2017

CREDC IAB Members

IAB Members
Exelon Utilities
Schweitzer Engineering Laboratories
Formerly of Chevron Corporation
Honeywell Building Solutions
Western Refining
North American Electric Reliability Corporation (NERC)
Electric Power Research Institute (EPRI)
Federal Energy Regulatory Commission (FERC)
Jet Propulsion Laboratory, Cyber Defense Engineering and Science Directorate
Idaho National Laboratory, National and Homeland Security (N&HS)

Opportunities to Engage with SEEDS

Event	Description	Location	Date
Project Validation Testing	Project technologies and tools will undergo validation testing to evaluate the potential for industry viability	TBD	TBD
Training Webinar	Training opportunity for researchers provided by an industry partner	Webinar	February 2017
SEEDS IAB Spring 2017 Meeting	SEEDS IAB members will convene to discuss SEEDS project activities	In-person location TBD	April 2017
SEEDS Industry Day	SEEDS will host event for researchers to discuss their activities with representatives from industry	TBD	Late 2017

SEEDS IAB Members

IAB Members	
Arkansas Electric Cooperative Corp. (AECC)	Kihomac
American Electric Power (AEP)	Leidos Cyber (past Lockheed Martin Industrial Defender, Inc.)
Bedrock Automation	Midcontinent Independent System Operator (MISO)
Brown Engineering	Netizen
Consolidated Edison of New York	OSI Soft
Entergy	Ozark Electric Cooperative Corp
Exelon	PJM Interconnection
FoxGuard Solutions	PPL Electric Utilities Corporation
Global Sign	Schweitzer Engineering Laboratories (SEL)
Kansas City Power and Light (KCPL)	Southwest Power Pool (SPP)

Transition to Practice – Academia

Indicates state where CEDS participation has resulted in technology transitioned to practice

TTP Example:
A research partnership led by the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) developed technology, called Amilyzer, that monitors AMI traffic, helping to ensure that smart meters are running in a secure state. (http://tcipg.org/amilyzer)

Emerging Successes Example:
Georgia Tech Research Institute (GTRI) is working on advanced power grid modeling that integrates the physics of power grid operations with the computer science of control systems. The partners include Burbank Water and Power, Cyber Technology and Information Systems Laboratory, Open Information Security Foundation, Southern Company, Strategic Energy Institute and Virgin Island Water and Power

Transition to Practice – Industry

Indicates state where CEDS participation has resulted in technology transitioned to practice

TTP Example:
Utilities in all 50 states in the United States have purchased technology Schweitzer Engineering Laboratories, Inc. (SEL) has developed and commercialized as part of projects in the CEDS cybersecurity program
A research partnership led by Schweitzer Engineering Laboratories (SEL) R&D has developed the first software defined network for more secure, reliable operational network traffic shaping – deny-by-default access control, and automatic, pre-defined rerouting around network disruption. (https://selinc.com/products/2740S/)

Emerging Successes Example:
A research partnership led by ABB enables protection and control devices to reach collaborative consensus as to whether a received command would support grid operations, or could be a malicious attempt to jeopardize grid stability. (http://energy.gov/sites/prod/files/2015/12/f27/CODEF%20fact%20sheet%20June%202015.pdf)

Transition to Practice – National Laboratories

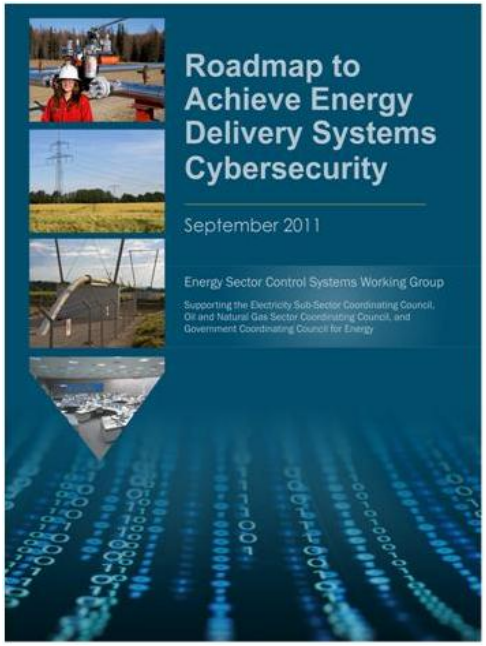
Indicates state where CEDS participation has resulted in technology transitioned to practice

TTP Example:
Oak Ridge National Laboratory (ORNL) licensed the Hyperion software technology to R&K Cyber Solutions LLC. Hyperion can look inside an executable program to determine its behavior without using the program's source code or running the program. (https://www.ornl.gov/news/hyperion-cyber-security-tech-receives-commercialization-award)

Emerging Successes Example:
The Quantum Security Modules for the Smart Grid project at Los Alamos advanced the state-of-the-art in secure communications for critical infrastructure protection. LANL scientists have reduced the facility footprint and improved the performance of their hybrid classical-quantum communications system.

For More Information, Please Contact:

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability



Carol Hawk
Program Manager
Cybersecurity for Energy Delivery Systems
Carol.Hawk@hq.doe.gov
202-586-3247

Visit:

http://energy.gov/oe/technology-development/control-systems-security