U.S. DEPARTMENT OF ENERGY

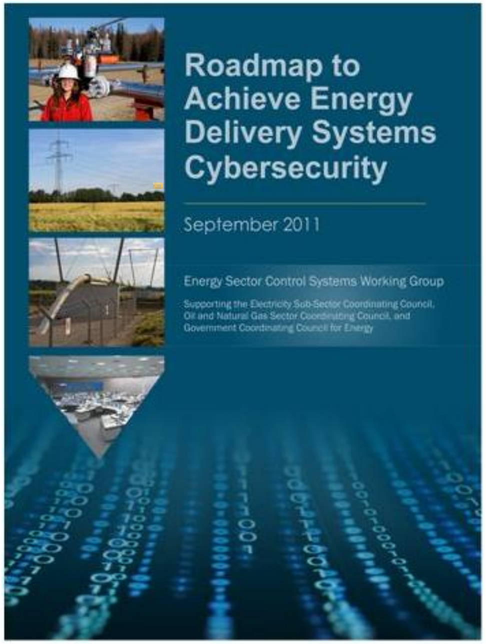
Office of
Electricity Delivery
& Energy Reliability

U.S. Department of Energy
Cybersecurity for Energy Delivery Systems

Dr. Carol Hawk

November 28, 2017

Roadmap – Framework for Collaboration



Roadmap to Achieve Energy Delivery Systems Cybersecurity

September 2011

Energy Sector Control Systems Working Group

Supporting the Electricity Sub-Sector Coordinating Council, Oil and Natural Gas Sector Coordinating Council, and Government Coordinating Council for Energy

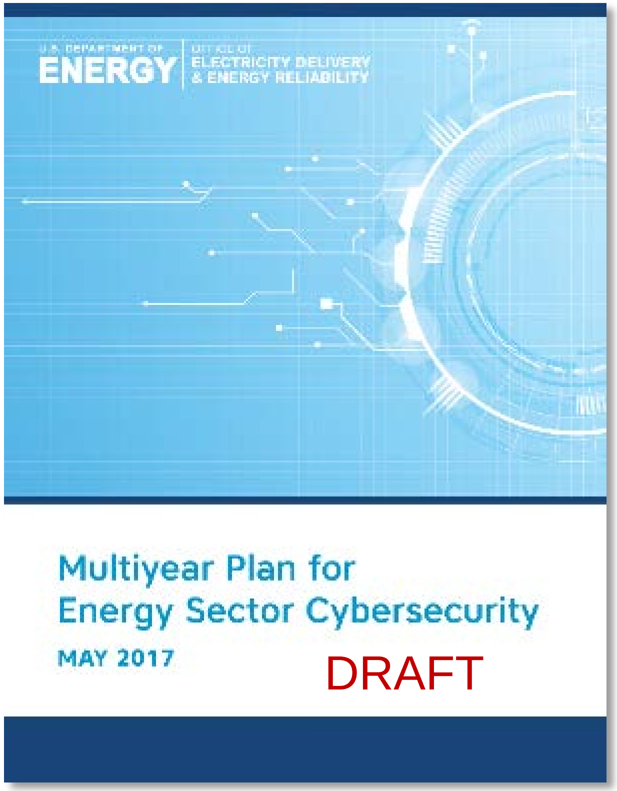
- *Energy Sector's* synthesis of energy delivery systems security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in energy delivery systems security

Roadmap Vision

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

For more information go to: https://energy.gov/oe/cybersecurity-critical-energy-infrastructure

DOE Multi-Year Plan for Energy Sector Cybersecurity



U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

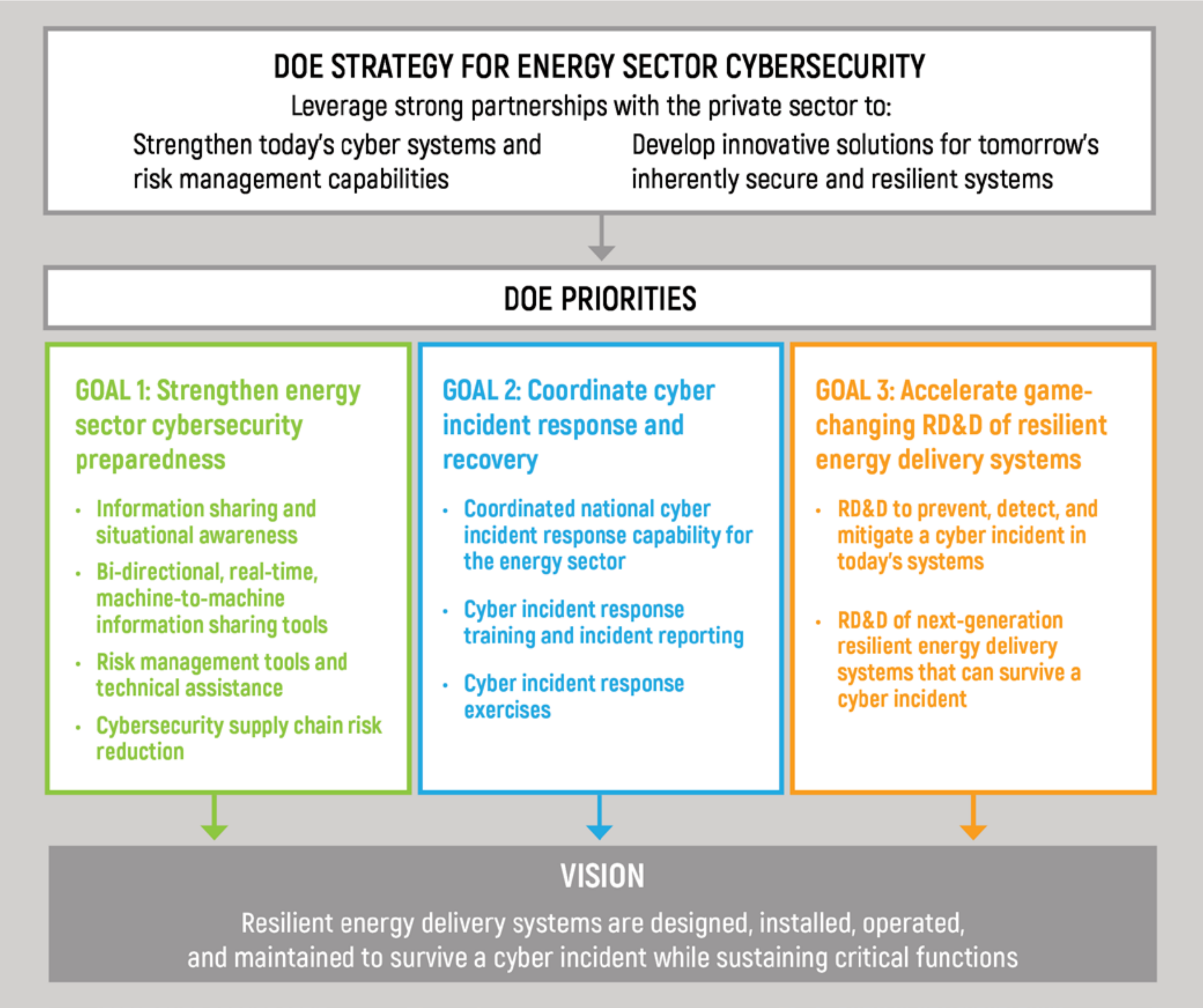
Multiyear Plan for Energy Sector Cybersecurity

MAY 2017

DRAFT

- **DOE's strategy** for partnering with industry to protect U.S. energy system from cyber risks
- **Guided by direct industry input** on cybersecurity needs and priorities
- **Market-based approach** encourages investment and cost-sharing of promising technologies and practices
- **Establishes goals, objectives, and performance targets** to improve both near- and long-term energy cybersecurity

DOE Strategy for Energy Sector Cybersecurity



DOE STRATEGY FOR ENERGY SECTOR CYBERSECURITY

Leverage strong partnerships with the private sector to:

Strengthen today's cyber systems and risk management capabilities

Develop innovative solutions for tomorrow's inherently secure and resilient systems

DOE PRIORITIES

GOAL 1: Strengthen energy sector cybersecurity preparedness

- Information sharing and situational awareness
- Bi-directional, real-time, machine-to-machine information sharing tools
- Risk management tools and technical assistance
- Cybersecurity supply chain risk reduction

GOAL 2: Coordinate cyber incident response and recovery

- Coordinated national cyber incident response capability for the energy sector
- Cyber incident response training and incident reporting
- Cyber incident response exercises

GOAL 3: Accelerate game-changing RD&D of resilient energy delivery systems

- RD&D to prevent, detect, and mitigate a cyber incident in today's systems
- RD&D of next-generation resilient energy delivery systems that can survive a cyber incident

VISION

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

GOAL 3: Accelerate Game-Changing RD&D of Resilient Energy Delivery Systems

PRIORITIES AND PATHWAYS

Research, develop, and demonstrate tools and technologies to:

1. **Prevent, detect, and mitigate cyber incidents in *today's energy delivery systems***
   - Decrease the cyber attack surface and block attempted misuse
   - Decrease the risk of malicious components inserted in the supply chain
   - Enable real-time, continuous cyber situational awareness
   - Automatically detect attempts to execute a function that could de-stabilize the system when the command is issued
   - Characterize cyber incident consequences and automate responses
2. **Change the game so that *tomorrow's resilient energy delivery systems* can survive a cyber incident**
   - Anticipate future grid scenarios and design cybersecurity into systems from the start
   - Enable power systems to automatically detect and reject a cyber attack, refusing any commands/actions that do not support grid stability
   - Build strategic partnerships and core capabilities in National Labs

Example Outcomes for Securing *Today's* Energy Delivery Systems

EXAMPLE OUTCOMES

Tools and technologies to *prevent* cyber attacks:

- → Quantum key distribution to securely exchange data using cryptographic keys while detecting attempted eavesdropping
- → Algorithms that continuously and autonomously assess and reduce the cyber attack surface

Tools and technologies to *detect* cyber attacks:

- → Rapid anomaly identification that may indicate a compromise in utility control communications
- → Tools to detect spoofing or compromise of the precise GPS time signals used for synchrophasor data

Example Outcomes for Securing *Today's* Energy Delivery Systems

EXAMPLE OUTCOMES

Tools and technologies to *mitigate* cyber attacks:

- → Ability for high-voltage DC systems to detect when commands could destabilize the grid and reject the command or take a different action
- → Network risk assessment model to classify attacks based on impact potential and assess network's resilience to zero-day attacks

Example Outcomes for *Tomorrow's* Resilient Energy Delivery Systems

EXAMPLE OUTCOMES

Tools and technologies to anticipate future grid scenarios, design in cybersecurity, and enable power systems to automatically recognize and reject a cyber attack:

- → Architectures that secure the cyber interaction of grid-edge devices and data streams in the cloud
- → Resilient building energy management systems that can switch to a more secure platform during a potential cyber incident
- → A cyber-physical control and protection architecture for multi-microgrid systems that enable stable grid performance during a cyber attack using electrical islands
- → Resilient operational networking technology that automates cyber incident responses

Build strategic core capabilities at 10 National Laboratories and build multi-university collaborations dedicated to advancing EDS cybersecurity

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
- FirstEnergy
- FP&L
- HECO
- Idaho Falls Power
- Inland Empire Energy
- NIPSCO
- Omaha Public Power District
- Orange & Rockland Utility
- Pacific Gas & Electric
- PacifiCorp
- 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
- Westar Energy
- 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
- Tenable Network Security
- 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

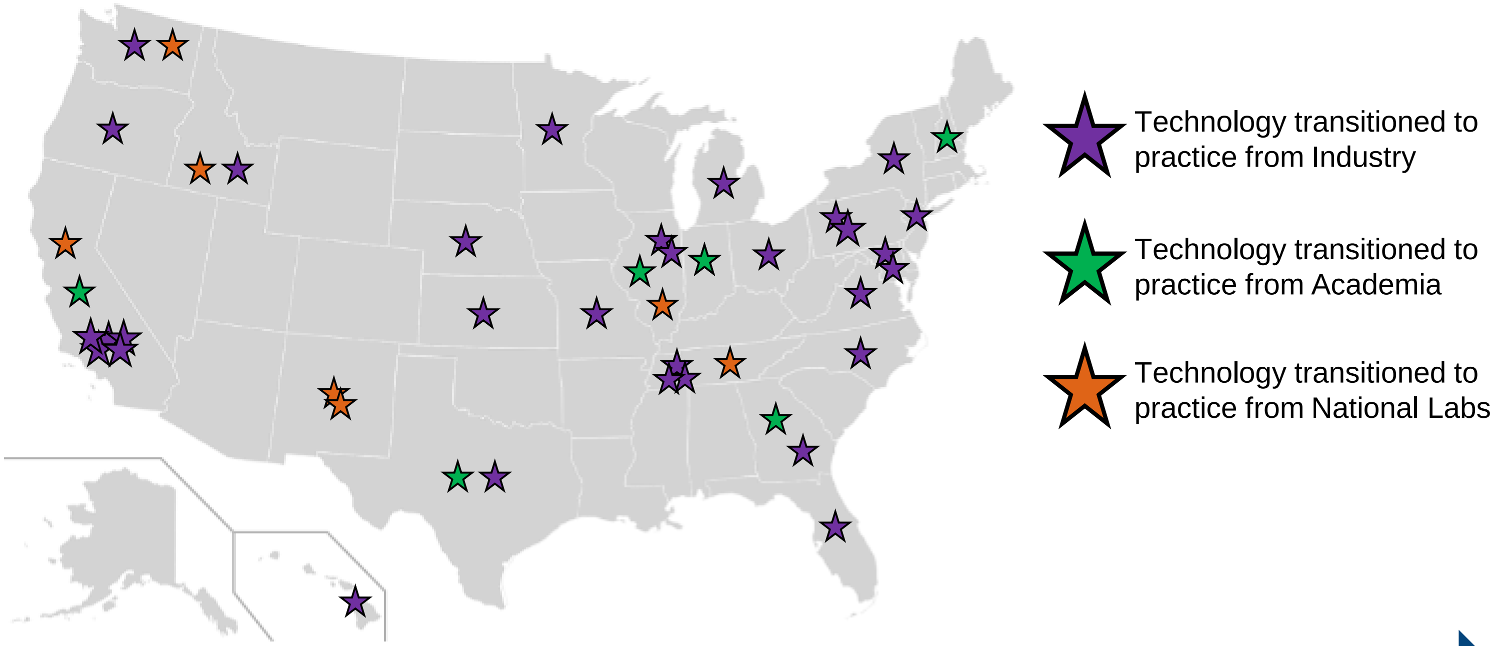
National Labs

- 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 Technologies Transitioned to Practice


★ Technology transitioned to practice from Industry
★ Technology transitioned to practice from Academia
★ Technology transitioned to practice from National Labs

DOE PIPELINE: Transition R&D to Practice in the Energy Sector

- CEDS R&D supports advanced technologies in the earlier, high-risk/high-reward research stages, for which a business case cannot readily be established by a private sector company and yet are needed to address a national security imperative

- Builds R&D pipeline through partnerships with energy sector utilities, vendors, universities, national laboratories, and providers of cybersecurity services to the energy sector

Results

- **Successfully transitioned more than 35 tools and technologies used TODAY** to help critical energy infrastructure survive a cyber incident

- **Approximately 1,000 utilities in 50 states have purchased technologies developed by CEDS**

FY2017 CEDS AOP Selections (1 of 6)

Argonne NATIONAL LABORATORY	Next-Generation Attack-Resilient Electricity Distribution Systems	Develop a cyber-attack-resilient architecture for next-generation electricity distribution systems that increase reliability by using distributed energy resources (DER) and microgrids.	ILLINOIS INSTITUTE OF TECHNOLOGY SMU ComEd. pjm EATON
INL Idaho National Laboratory	(FIT) Firmware Indicator Translation	Develop techniques to translate indicators of compromise that may have initially been developed for use by IT desk-top systems, so they can be more effectively used for OT operational networks to help secure firmware on the embedded systems used by energy sector field devices.	SOUTHERN CALIFORNIA EDISON wfec western farmers electric cooperative Pacific Northwest NATIONAL LABORATORY AIR FORCE FELLOWS BYU Idaho State UNIVERSITY
BERKELEY LAB	Adaptive Control of Electric Grid Components for Cyber-Resiliency	Enable distribution grids to adapt to resist a cyber-attack by (1) developing adaptive control algorithms for DER, voltage regulation, and protection systems; (2) analyze new attack scenarios and develop associated defensive strategies.	OSIsoft. SUNSPEC ALLIANCE solaredge PSL HDPV ALLIANCE ASU Arizona State University NRECA SMUD EPRI SIEMENS

FY2017 CEDS AOP Selections (2 of 6)

Cyber Interconnection Analysis for High Penetration of DER

Develop a tool that can evaluate cyber-risk, and design remediation strategies to survive a cyber-attack, for a distribution-level power grid that uses a high penetration of DER to enhance reliability.

Hawaiian Electric
RS Revolutionary Security
EATON
solaredge
City of Riverside Public Utilities
OSIsoft.
PSL
smarter grid solutions

GPS Interference Detection

Develop a technology to rapidly detect interference of precise synchronized time signals used by phasor measurement units (PMUs) for wide area situational awareness of power grid operations.

SDGE
PSL

Secure SCADA Protocol Characterization and Standardization

Advance SSP21 (Secure SCADA Protocol for the 21st Century) through development of an industrial key infrastructure (IKI) to help protect energy infrastructure information by easing the process of cryptographic key exchange.

Sempra Energy
SDGE
EATON

Los Alamos
NATIONAL LABORATORY

Quantum Key Distribution for the Energy Sector: Trusted Node Relays and Networks

Research, design and prototype a quantum secure communication (QSC) operational network, including trustworthy relays to extend distance and decrease cost, for critical energy infrastructure.

OAK RIDGE
National Laboratory

FY2017 CEDS AOP Selections (3 of 6)

NREL NATIONAL RENEWABLE ENERGY LABORATORY	(Module-OT): Modular Security Apparatus for Managing Distributed Cryptography for Command & Control Messages on Operational Technology (OT) Networks	Develop a lower-cost distributed cryptography technique to help protect energy infrastructure information, in particular, the operational networks used for command and control of DER that are being increasingly used to enhance power grid reliability.	SEL SCHWEITZER ENGINEERING LABORATORIES PNM Sandia National Laboratories
OAK RIDGE National Laboratory	Darknet	Define the requirements for a secure energy delivery control system network that is independent of the public internet, and uses existing but currently unused optical fiber, so called "dark fiber".	**Multiple universities and power providers**
OAK RIDGE National Laboratory	Quantum Physics Secured Communications for the Energy Sector	Decrease cost, and increase distance, of Quantum Key Distribution systems that enable real-time detection of adversarial intrusion on control system networks.	Los Alamos NATIONAL LABORATORY epb Qubitekk SDGE
OAK RIDGE National Laboratory	Energy Delivery Systems with Verifiable Trustworthiness	Provide a tool to verify the integrity of firmware used in energy delivery system devices, without taking the equipment offline.	NRECA epb ISA Security Compliance Institute Schneider Electric TVA

FY2017 CEDS AOP Selections (4 of 6)

Oak Ridge National Laboratory	Malware Mitigation for Energy Delivery Systems (MMEDS)	Work with energy sector partners to mitigate cyber-risk in energy delivery systems and components.	University of Illinois The University of Tennessee Knoxville University of Nebraska Lincoln MIT epb Duke Energy TVA ISA Security Compliance Institute Schneider Electric
Pacific Northwest National Laboratory	KISS (Keyless Infrastructure Security Solution)	Develop block-chain cybersecurity technology for distributed energy resources at the grid's edge, such as transactive energy exchanges that can be expected to create new markets.	Washington State University Siemens TVA HDIAC Homeland Defense & Security Information Analysis Center guardtime
Pacific Northwest National Laboratory	MEEDS (Mitigation of External-exposure of Energy Delivery System Equipment)	Develop a tool for use by a utility or energy asset owner/operator, to identify their energy delivery system equipment that may have been inadvertently exposed to the public internet and mitigate associated risk.	NRECA tenable network security P.U.D. Chelan County

FY2017 CEDS AOP Selections (5 of 6)

Pacific Northwest NATIONAL LABORATORY

SASS-E (Safe & Secure Autonomous Scanning Solution for Energy Delivery Systems)

Develop scanning methodologies, models, and architectures to transform a network vulnerability scanner widely deployed in the IT space, into a scanner that can be used in the operational technology (OT) networks of critical energy infrastructure where legacy equipment may respond unpredictably when subjected to active scanning techniques often used in IT.

NRECA P.U.D. CHELAN COUNTY SIEMENS tenable network security

Pacific Northwest NATIONAL LABORATORY

SDN4EDS (Software Defined Networking for Energy Delivery Systems)

Develop a comprehensive blueprint and secure reference architecture to ease the process of deploying software defined networking (SDN) technology to better secure operational networks throughout the energy sector.

NREL NATIONAL RENEWABLE ENERGY LABORATORY Sandia National Laboratories California ISO SOUTHERN CALIFORNIA EDISON SEL SCHWEITZER ENGINEERING LABORATORIES JUNIPER NETWORKS dispersive technologies

Pacific Northwest NATIONAL LABORATORY

UUDEX (Universal Utility Data Exchange)

Develop a secure and flexible data exchange approach for communication between control centers, including Inter-Control Center Communications Protocol (ICCP) data exchanges.

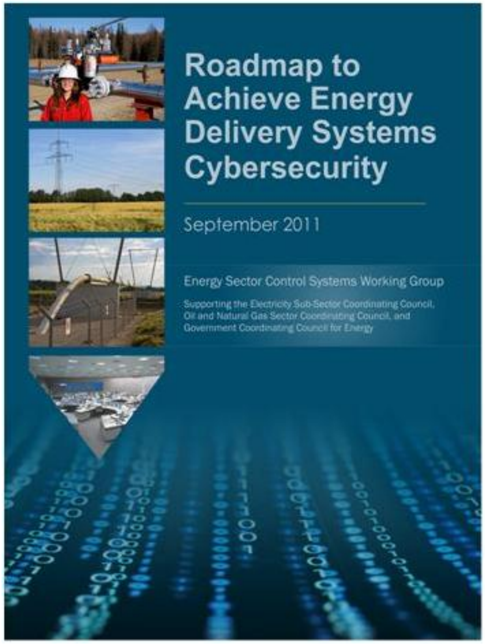
OATI MITRE

FY2017 CEDS AOP Selections (6 of 6)

Pacific Northwest National Laboratory	MICE (Malware Identification and Containment for EDS)	Build partnership among suppliers and end users of energy delivery infrastructure components and systems to reduce cyber-risk.	GE SEL Schweitzer Engineering Laboratories Siemens soteria cyber security MVEC Minnesota Valley Electric Cooperative Red Trident Inc South River Electric Membership Corporation
Sandia National Laboratories	Containerized Application Security for Industrial Control Systems	This project will increase the availability and resiliency of control systems by dynamically migrating, updating and restoring applications during a cyber incident.	SEL Schweitzer Engineering Laboratories Pacific Northwest National Laboratory Chevron Fort Belvoir Sempra Energy GRIMM
Sandia National Laboratories	Survivable Industrial Control System	This project will develop technology that proactively detects adversarial manipulation of power system equipment by, for example, checking that received commands support grid stability, and appropriately respond by, for example, reconfiguring the operational network to isolate, then eradicate, the intrusion while sustaining critical energy delivery functions.	SEL Schweitzer Engineering Laboratories Pacific Northwest National Laboratory Georgia Tech GRIMM Chevron Fort Belvoir Sempra Energy

For More Information, Please Contact:

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



Roadmap to Achieve Energy Delivery Systems Cybersecurity

September 2011

Energy Sector Control Systems Working Group

Supporting the Electricity Sub-Sector Coordinating Council, Oil and Natural Gas Sector Coordinating Council, and Government Coordinating Council for Energy

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

Visit:

https://energy.gov/oe/cybersecurity-critical-energy-infrastructure