U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

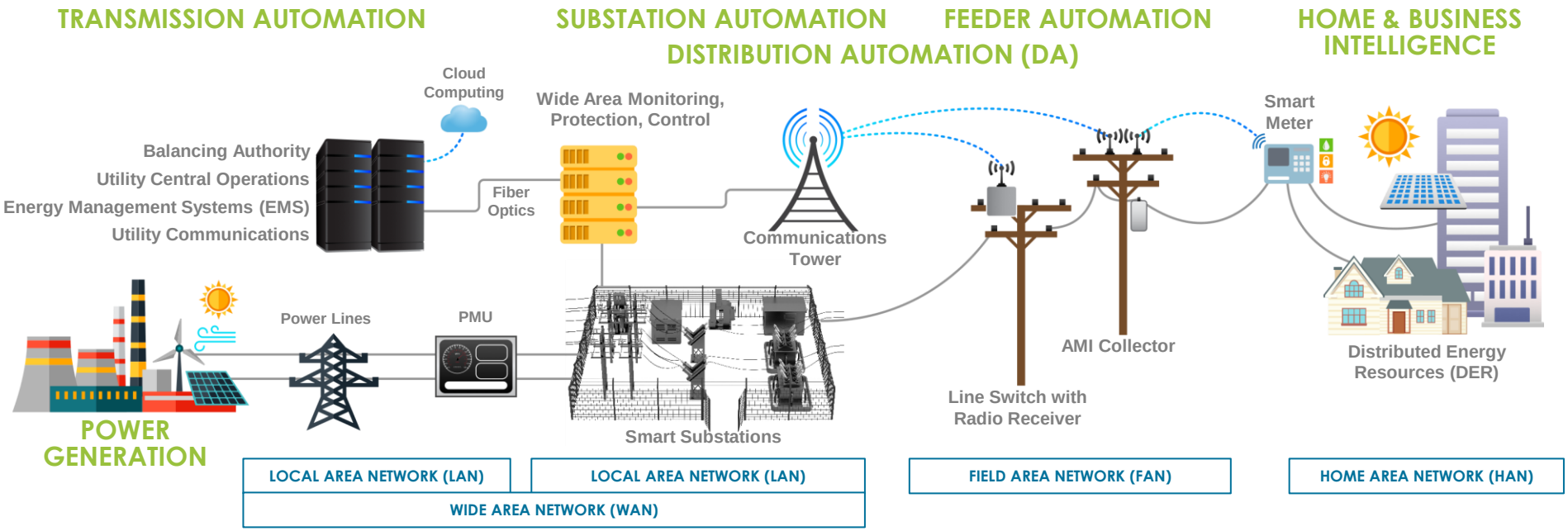
Cybersecurity for Energy Delivery Systems (CEDS) Division Overview

Carol Hawk

Acting Deputy Assistant Secretary

November 8, 2018

Electricity Delivery Infrastructure



Operational Technology (OT) and Information Technology (IT)

Energy delivery control systems are OT:

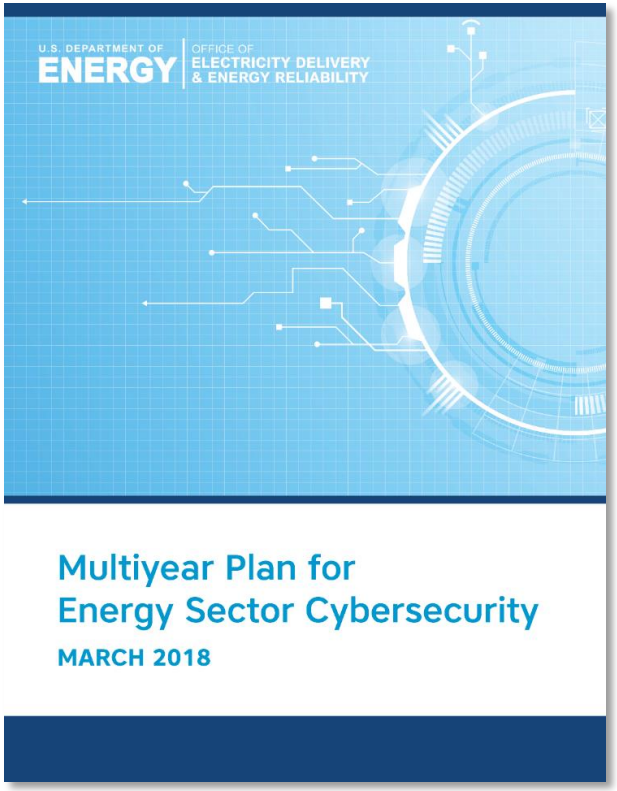
- Computers and networks that manage, monitor, protect and control energy delivery
- Cyber-attack can disrupt power, damage physical equipment, jeopardize public safety, economic prosperity and national security

Energy delivery cybersecurity OT solutions must be tailored to support operations

- No down time for system fixes – power systems must operate 24/7 with high reliability and high availability
- Components are distributed over wide geographical regions, publicly accessible subject to tampering
- Legacy equipment and protocols not designed to support cybersecurity measures
- Latency is often unacceptable – cyber solutions cannot slow system operations
- Active scanning of network can interfere with equipment operations
- Real-time emergency response capability is necessary
- Patches/upgrades require rigorous, prolonged testing

Physics Rules OT

DOE CESER Multiyear Plan for Energy Sector Cybersecurity

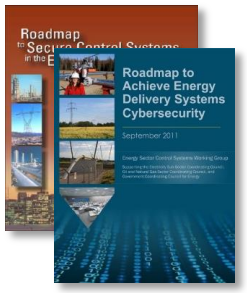


- **DOE's strategy** for partnering with industry to protect U.S. energy system from cyber risks
- **Guided by direct industry input** on cybersecurity needs and priorities – complements the Energy Sector Roadmap
- **Market-based approach** encourages investment and cost-sharing of promising technologies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

CEDS Vision

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

MYP Supports Government and Private Sector Priorities for Energy Sector Cybersecurity



Energy Sector Control Systems Roadmaps

Presidential Policy Directives

- PPD-21 and PPD-41

Executive Orders

- E.O. 13636 and E.O. 13800

EISA, 2007

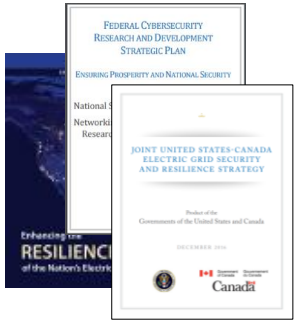
FAST Act, 2015

Federal Policies

Multiyear Plan for Energy Sector Cybersecurity

- Electricity Advisory Council
- Electricity Sector Coordinating Council
- Oil and Natural Gas Sector Coordinating Council
- Grid Modernization Lab Consortium

Energy Sector Stakeholders



Federal Strategies and Reports

DOE's Strategy for Energy Sector Cybersecurity

Leverage strong partnerships with the energy sector to:

1 **Strengthen today's cyber systems and risk management capabilities**

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

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

- Coordinate national cyber incident response for the energy sector
- Build cyber incident response 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
- Build National Lab core capabilities and university collaborations

MYP 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

140+ Partners Participating in CEDS R&D

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
- TDi Technologies
- 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

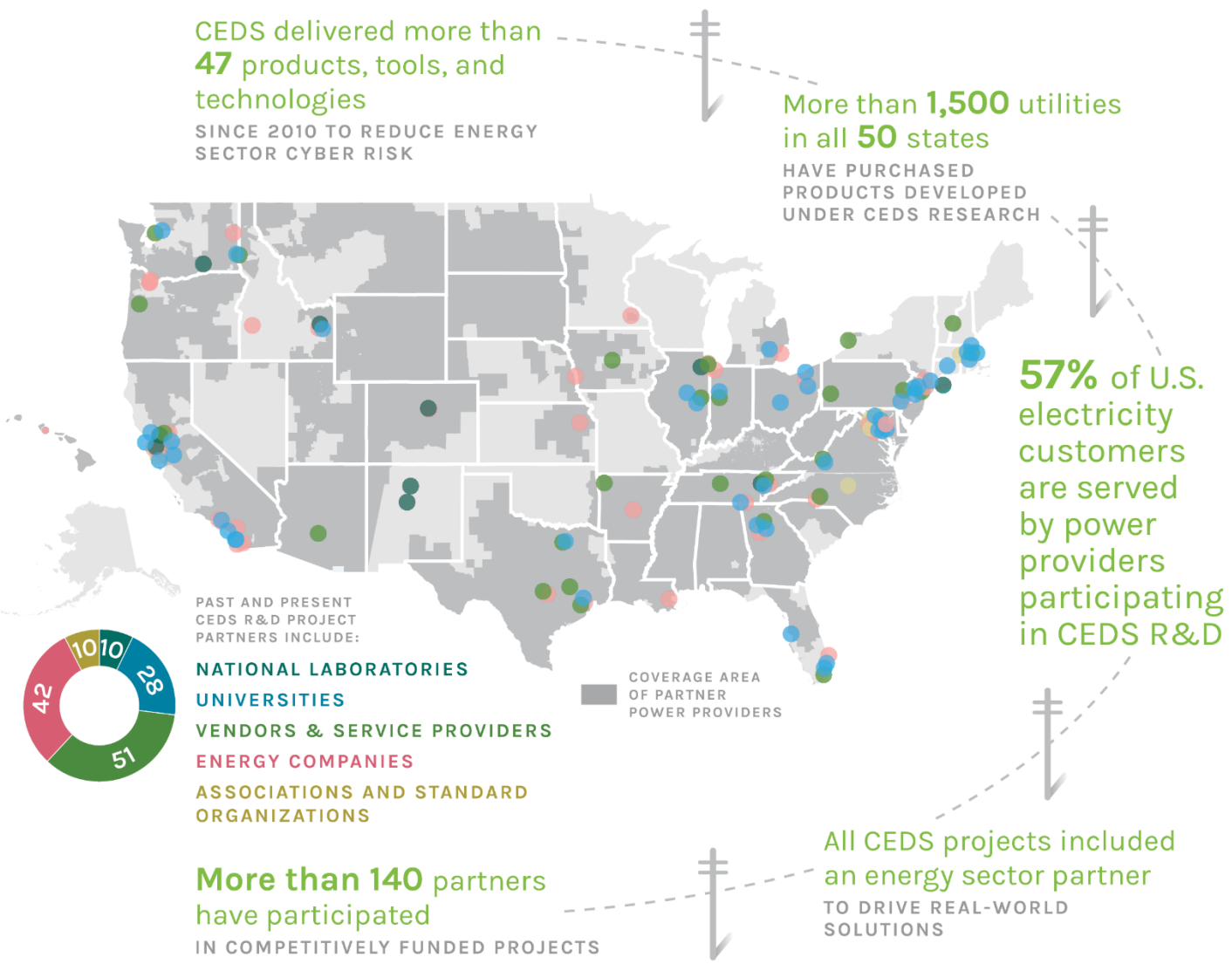
- Argonne National Laboratory
- Brookhaven National Laboratory
- Idaho National Laboratory
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- National Renewable Energy Laboratory
- Oak Ridge National Laboratory
- Pacific Northwest National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

Other

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

CEDS R&D Reach and Impact

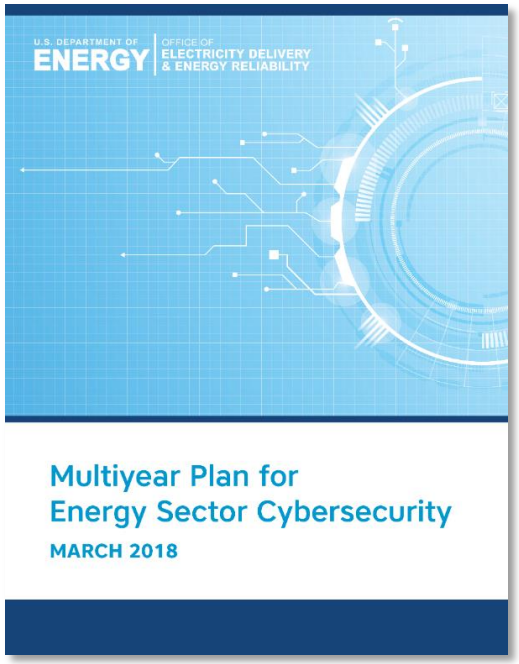
- **Funds earlier, high-risk/high-reward R&D** in areas critical for national security where a business case cannot readily be established by a private-sector company
- **Builds R&D pipeline through partnerships** with energy sector utilities, vendors and service providers, universities, and national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



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)

For More Information, Please Contact:



Dr. Carol Hawk
Acting Deputy Assistant Secretary
Cybersecurity for Energy Delivery Systems (CEDS) Division
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Carol.Hawk@hq.doe.gov
202-586-3247

Visit: https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response