DOE Strategy for Energy Sector Cybersecurity

Hank Kenchington
Deputy Assistant Secretary, Cybersecurity and Emerging Threats R&D
September 14, 2017
## Energy Sector Partners Are Critical to Success

**Asset Owners/Operators (36)**
- 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 (35)**
- ABB
- Alstom Grid
- Applied Communication Services
- Applied Control Solutions
- Cigital, Inc.
- Critical Intelligence
- Cybati
- Eaton
- Enernex
- EPRI
- Foxguard
- 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 (23)**
- 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 (10)**
- 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 (5)**
- Energy Sector Control Systems Working Group
- International Society of Automation
- NESCOR
- NRECA
- Open Information Security Foundation

109 public-private partners drive R&D
• **Energy Sector’s** synthesis of critical control system security challenges, R&D needs, and implementation milestones

• Provides strategic framework to:
  - Ensure public and private R&D is relevant and meets the needs of energy utilities
  - Stimulate investments in control systems security

**Roadmap Vision**
Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions
## Roadmap Milestones and Goals

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.1 Executive Engagement and support of cyber resilience efforts</td>
<td>1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available</td>
<td>1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry</td>
<td>1. Assess and Monitor Risk</td>
<td>2. Manage Incidents</td>
<td>3. Develop and Implement New Protective Measures to Reduce Risk</td>
<td>4. Manage Incidents</td>
<td>5. Sustain Security Improvements</td>
</tr>
<tr>
<td></td>
<td>Industry-driven safe code development and software assurance awareness workforce training campaign launched</td>
<td>1.4 Field-proven best practices for energy delivery systems security widely employed</td>
<td>1.5 Compelling business case developed for investment in energy delivery systems security</td>
<td></td>
<td>2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings</td>
<td>3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available</td>
<td>4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available</td>
<td>5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics</td>
<td></td>
<td></td>
<td>3.2 Scalable access control for all energy delivery system devices available</td>
<td>3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented</td>
<td>4.2 Tools to support and implement cyber-attack response decision making for the human operator commercially available</td>
<td>5.2 Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available</td>
<td>3.4 Self-configuring energy delivery system network architectures widely available</td>
<td>3.5 Capabilities that enable security solutions to continue operation during a cyber-attack available as upgrades and built-in to new security solutions</td>
<td>4.3 Incident reporting guidelines accepted and implemented by each energy subsector</td>
<td>5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented</td>
<td>4.4 Real-time forensics capabilities commercially available</td>
<td>4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available</td>
<td>5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.4 Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators</td>
<td>3.7 Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment</td>
<td>4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector</td>
<td>5.5 Private-sector investment surpasses federal investment in developing cybersecurity solutions for energy delivery systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Next-generation energy delivery system architectures provide &quot;defense in depth&quot; and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident</td>
<td>3.8 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders are commercially available</td>
<td>4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available</td>
<td>5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment</td>
<td></td>
<td>5.7 Collaboration between industry, academia, and government maintains cybersecurity advances</td>
<td></td>
</tr>
</tbody>
</table>
### Ongoing Projects

<table>
<thead>
<tr>
<th>OE-Funded RD&amp;D Portfolio</th>
<th>Industry-Defined Roadmap Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microgrid Assets</strong></td>
<td></td>
</tr>
<tr>
<td>Texas A&amp;M Engineering Experiment Station: “Timing Intrusion Management Ensuring Resilience (TIMER)”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory (SNL): “Artificial Diversity Assessment”</td>
<td></td>
</tr>
<tr>
<td>Lawrence Livermore National Laboratory (LLNL): “Scalable Security Monitoring and Compliance Measure”</td>
<td></td>
</tr>
<tr>
<td>Lawrence Berkeley National Laboratory: “Detecting the Energy Sector Operations”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois: “Modeling Security for Grid Automation”</td>
<td></td>
</tr>
<tr>
<td>University of Arkansas: “Detecting Delivery Systems”</td>
<td></td>
</tr>
<tr>
<td>Intel Federal, LLC: “Enhanced Security for the System Edge”</td>
<td></td>
</tr>
<tr>
<td>ABB, Inc.: “Cyber Attack Resilient HVDC System”</td>
<td></td>
</tr>
<tr>
<td>ABB, Inc.: “Multi-layered Resilient Microgrid”</td>
<td></td>
</tr>
<tr>
<td>United Technologies Research Center “Portaledge”</td>
<td></td>
</tr>
<tr>
<td>ABB, Inc.: “Microgrid Assets”</td>
<td></td>
</tr>
</tbody>
</table>

### Completed Foundational Projects (Goal 3 Successes)

<table>
<thead>
<tr>
<th>OE-Funded RD&amp;D Portfolio</th>
<th>Industry-Defined Roadmap Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microgrid Assets</strong></td>
<td></td>
</tr>
<tr>
<td>University of Arkansas: “Detecting Devices”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois at Urbana-Champaign: “Cybersecurity Incidents in Energy Electricity”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois at Urbana-Champaign: “Cyber-Physical Analysis for Cyber-Physical Systems”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois: “Understanding the Special Case of Digital Forensics in Energy Delivery Systems”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory (SNL): “Artificial Diversity and Defense Security (ADDSeC)”</td>
<td></td>
</tr>
<tr>
<td>Idaho National Laboratory (INL): “High Level Language Microcontrollers”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory: “Trust Anchor/CodeSeal”</td>
<td></td>
</tr>
</tbody>
</table>

### Ongoing Projects

<table>
<thead>
<tr>
<th>OE-Funded RD&amp;D Portfolio</th>
<th>Industry-Defined Roadmap Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microgrid Assets</strong></td>
<td></td>
</tr>
<tr>
<td>University of Illinois: “Modeling Security for Grid Automation”</td>
<td></td>
</tr>
<tr>
<td>University of Arkansas: “Detecting Delivery Systems”</td>
<td></td>
</tr>
<tr>
<td>Intel Federal, LLC: “Enhanced Security for the System Edge”</td>
<td></td>
</tr>
<tr>
<td>ABB, Inc.: “Cyber Attack Resilient HVDC System”</td>
<td></td>
</tr>
<tr>
<td>ABB, Inc.: “Multi-layered Resilient Microgrid”</td>
<td></td>
</tr>
<tr>
<td>United Technologies Research Center “Portaledge”</td>
<td></td>
</tr>
<tr>
<td>ABB, Inc.: “Microgrid Assets”</td>
<td></td>
</tr>
</tbody>
</table>

### Completed Foundational Projects (Goal 3 Successes)

<table>
<thead>
<tr>
<th>OE-Funded RD&amp;D Portfolio</th>
<th>Industry-Defined Roadmap Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microgrid Assets</strong></td>
<td></td>
</tr>
<tr>
<td>University of Arkansas: “Detecting Devices”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois at Urbana-Champaign: “Cybersecurity Incidents in Energy Electricity”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois at Urbana-Champaign: “Cyber-Physical Analysis for Cyber-Physical Systems”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois: “Understanding the Special Case of Digital Forensics in Energy Delivery Systems”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory (SNL): “Artificial Diversity and Defense Security (ADDSeC)”</td>
<td></td>
</tr>
<tr>
<td>Idaho National Laboratory (INL): “High Level Language Microcontrollers”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory: “Trust Anchor/CodeSeal”</td>
<td></td>
</tr>
</tbody>
</table>

### OE-Funded RD&D Portfolio

<table>
<thead>
<tr>
<th><strong>Microgrid Assets</strong></th>
<th>Industry-Defined Roadmap Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Arkansas: “Detecting Devices”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois at Urbana-Champaign: “Cybersecurity Incidents in Energy Electricity”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois at Urbana-Champaign: “Cyber-Physical Analysis for Cyber-Physical Systems”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois: “Understanding the Special Case of Digital Forensics in Energy Delivery Systems”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory (SNL): “Artificial Diversity and Defense Security (ADDSeC)”</td>
<td></td>
</tr>
<tr>
<td>Idaho National Laboratory (INL): “High Level Language Microcontrollers”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory: “Trust Anchor/CodeSeal”</td>
<td></td>
</tr>
</tbody>
</table>

### Industry-Defined Roadmap Milestones

<table>
<thead>
<tr>
<th><strong>Microgrid Assets</strong></th>
<th>Industry-Defined Roadmap Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Arkansas: “Detecting Devices”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois at Urbana-Champaign: “Cybersecurity Incidents in Energy Electricity”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois at Urbana-Champaign: “Cyber-Physical Analysis for Cyber-Physical Systems”</td>
<td></td>
</tr>
<tr>
<td>University of Illinois: “Understanding the Special Case of Digital Forensics in Energy Delivery Systems”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory (SNL): “Artificial Diversity and Defense Security (ADDSeC)”</td>
<td></td>
</tr>
<tr>
<td>Idaho National Laboratory (INL): “High Level Language Microcontrollers”</td>
<td></td>
</tr>
<tr>
<td>Sandia National Laboratory: “Trust Anchor/CodeSeal”</td>
<td></td>
</tr>
</tbody>
</table>
Energy Sector: A Major Target of Cyber Attacks

- Aggressive attacks are outpacing defense
- Growing attack surface of U.S. energy infrastructure
- Public examples of attacks on foreign ICS demonstrate attack knowledge (Ukraine)

Cyber Incidents Reported to DHS ICS-CERT (2013-2015)
Total Reported Incidents: 796

- Critical Manufacturing: 26%
- Water: 6%
- Transportation: 6%
- Communications: 4%
- Healthcare: 4%
- Government Facilities: 5%
- All Others: 14%
- Energy: 35%

More Targeted and Sophisticated Attacks

**SHODAN**  
Developed in 2009  
- Search engine to find Internet-connected devices (including control system field devices)  
- Increase in IoT devices increases potential exploits

**METASPLOIT**  
October 2010 – First SCADA exploit  
- Open-source penetration testing tool developed in 2003 to expose vulnerabilities  
- First modules to exploit control system devices (PCS and SCADA) released 2011

**STUXNET**  
July 2010  
- Advanced persistent threat (APT) attack on SCADA control systems in Iranian nuclear centrifuge facilities  
- Relied on zero-day exploits  
- OT centrifuge equipment irreparably damaged by operating out of bounds

**SHAMOON**  
August 2012  
- Virus destroys data on workstations as means to disrupt operations  
- 2012 weaponized malware hit 15 state bodies and private companies in Saudi Arabia, wiping >35,000 hard drives of Aramco oil supplier  
- Iranian-backed hackers suspected  
- 2017 version hit 3 state agencies and 4 private-sector companies in Saudi Arabia

**UKRAINE POWER GRID**  
December 2015  
- 225,000 customers lost power in coordinated attack  
- SCADA systems targeted and damaged  
- Military-like planning and execution  
- Utility companies infiltrated 9 months prior to attack  
- Launched with easily available attack tools (malware and denial of service)
Electricity Delivery System is Evolving to Meet Customer Needs and Changing Generation Mix

**HISTORICAL**
- Human-based grid management
- Centralized generation/control
- One-way power and info flow

**EMERGING**
- Increasing distributed generation/control
- Multi-level coordination
- Increasing reliance on sensors and information and control technologies (ICT)
- Two-way power and info flow

Graphic Source: International Energy Agency
• **DOE’s strategy/plan** for partnering with industry to enhance cybersecurity of U.S. energy system

• **Guided by direct industry input** on cybersecurity needs and priorities – complements the 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
Energy Sector Needs inform DOE Strategy

Industry Priorities

- Roadmap to Achieve Energy Delivery Systems Cybersecurity (2011)
- Roadmap Assessment (2016)
- Consultation with Electricity and Oil and Natural Gas Subsector Councils

Federal Policies

- EO 13636, Improving Critical Infrastructure Cybersecurity (2013)
- PPD-21, Critical Infrastructure Security and Resilience (2013)
- Energy Security (Division F of the FAST Act) (2015)
- PPD-41, US Cyber Incident Coordination (2016)
- EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017)

Federal Strategies

- Federal Cybersecurity Research and Development Strategic Plan (2016)

DOE Multiyear Plan for Energy Sector Cybersecurity

Plan Implementation
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**
   - 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

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

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
GOAL 1: Strengthen Energy Sector Cybersecurity Preparedness

PRIORITIES AND EXAMPLE OUTCOMES

1. **Enhanced situational awareness and information sharing**
   → Sensors to capture OT data for electricity and oil and natural gas, private-sector clearances, and intelligence information sharing

2. **Real-time, machine-to-machine cyber defense**
   → Distributed malware analysis platform that safely enables automated and manual analysis of malicious code

3. **Risk management tools, guidelines, and training**
   → Enhance state-federal coordination (Energy Assurance Plans) and planning (exercises and workforce), and update Cybersecurity Capability Maturity Model (C2M2); expand oil and gas emphasis

4. **Improved understanding of cyber supply chain risks**
   → Collaborative public-private partnerships to gain insight into systemic vulnerabilities
Cybersecurity Risk Information Sharing Program (CRISP)

Identify threat patterns across the electric industry by analyzing real-time traffic using U.S. Intelligence capabilities

**Approach**

- Unique platform enables energy companies to voluntarily share IT network data
- Delivers cyber threat information – enriched with intelligence insights and tools – to help identify malicious activity and prioritize mitigation

**Industry Impact**

- Participating utilities account for ~75% of U.S. electric customers
- Developed by DOE and transitioned to the E-ISAC starting in 2014
- Allows IT data sharing for threat mitigation

CRISP is now managed by the Electricity – Information Sharing and Analysis Center (E-ISAC)
Advanced Tools to Enhance Threat Detection and Information Sharing

Cyber Analytics Tools and Techniques (CATT)

- Improve the speed, value, and cost of CRISP analysis, reports, and mitigations
- Improve IT threat detection by adding new analytic tools and capabilities to CRISP platform (working with PNNL, INL, ORNL, ANL)
- Better leverage U.S. Intelligence by enabling direct analysis of CRISP data in secure government storage using unique and sophisticated intelligence tools

CYbersecurity for the Operational Technology Environment (CYOTE)

- Pilot a two-way OT data sharing and analysis capability (similar to CRISP) with 4 utilities for the complex OT environment – where threat monitoring and detection is not widespread
- Map the OT cyber “kill chain” – the attack pathways hackers could use to compromise utility OT systems
- Identify OT network sensors that monitor the right data and meet demanding OT network requirements
Working With Small and Medium-Sized Utilities (over 2,000) to Enhance Cybersecurity

Program Objectives
• Engage with public power distribution utilities to better understand cyber security posture and implement programs to improve

Industry Impact
• Support smaller distribution utilities that typically have limited resources invest in cyber resilience and stay ahead of rapidly evolving sophisticated cyber threats

Approach
• Work through leading trade associations to provide resources, training, and technical assistance to member utilities
• Conduct cyber security risk assessments
• Conduct onsite vulnerability assessments
• Pilot existing or emerging cybersecurity technologies
• improve/develop process to better share threat information

Partners

APPA – Trade association for >2,000 local- and state-owned utilities serving >48 million Americans
• APPA partners include Axio and Energetics, Inc.

NRECA – Trade association for >900 not-for-profit rural electric cooperatives and public power districts serving >42 million customers in 47 states
• R3C – The Rural Cooperative Cyber Security Capabilities Program
• Partners include Cigital and BlackByte Cyber Security LLC
Cybersecurity Capability Maturity Model (C2M2)

- Public-private partnership program to help energy sector asset owners and operators assess their capabilities and continuously improve their cybersecurity posture.

- C2M2 strengthens organizational cybersecurity capabilities; shares best practices, and employs the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

- The C2M2 helps organizations – regardless of size, type, or industry to evaluate, prioritize, and improve their own cybersecurity capabilities.

Executive Order 13636 Improving Critical Infrastructure Cybersecurity
Section 8(b)

"Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."
GOAL 2: Coordinate Cyber Incident Response and Recovery

1. Coordinated national cyber incident response for the energy sector
   • Fulfill our SSA responsibilities
   • Educate stakeholders on processes, roles, responsibilities, and resources; integrated into the DOE unified command structure

2. Build additional Cyber incident response capability
   • Build energy specific OT teams and capability to support cyber incident response
   • ESF-12 responders across the nation trained on coordination needs for intersection of cyber incidents and physical response through FEMA
   • Improve cyber incident reporting process for private-sector partners

3. Annual cyber incident response exercises with industry and federal/state/local stakeholders
DOE Cyber Response Partnership (CRP) Teams

Vision: Mission-ready access to energy sector specific cybersecurity expertise, capabilities, and resources for cyber incident response

- Deliver expert assistance to industry cyber victims
- Establish energy sector cyber response structure and processes
- Agreements in place with 5 National Labs
- Scalable technical assistance capability
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
Cybersecurity for Energy Delivery Systems (CEDS) R&D Program Approach

**Long-Term, Foundational Projects**
- Core and Frontier National Laboratory Research Program
- Academia Projects

**Mid-Term Projects**
- National Laboratory Led Projects

**Shorter-Term Projects**
- Energy Sector Led Projects

**GOAL: Transition R&D to Practice in the Energy Sector**

- Funds innovative R&D in areas critical for national security where the industry lacks a clear business case
- Builds R&D pipeline through partnerships with energy sector utilities, suppliers, universities and national laboratories
- Successfully transitioned more than 30 tools and technologies used TODAY to better secure U.S. energy infrastructure
- Over 990 utilities in 50 states have purchased technologies developed by CEDS
R&D Successes Include Advanced Technologies That Enhance Cybersecurity AND Lower Operating Costs

Commercially Available in FY16

Software Defined Networking (SDN):

- Monitors network traffic using a whitelist approach and quarantines unauthorized or suspicious devices
- Improves network performance with <100uS network heal times
- Market-ready solution resulting from strong partnerships and real-world demonstration

SEL-led research partnership with:
- Pacific Northwest National Laboratory (PNNL)
- University of Illinois at Urbana Champaign
- Ameren

Reference: UTC Journal, 3rd Quarter 2016
Cybersecurity Intrusion Detection and Monitoring for Field Area Networks

- Detects anomalies and attacks in smart grid wireless mesh networks for smart meters and distribution automation
- Demonstrated at 4 utilities and commercialized as SecureSmart technology
- Now used today to give operators great visibility into critical smart grid networks
- Deployments -

---

**PROJECT LEAD**

**PARTNER**
Using Physics of Electric Power Flow to Thwart Cyber Attacks

**CODEF – Collaborative Defense of Transmission and Distribution Protection and Control Devices**

- Automatically detects and rejects malicious commands that could jeopardize physical grid operations if acted on
- Anticipates the effects of each command and only enacts those that will **support grid stability**
- Demonstrated transmission level cybersecurity functions at Bonneville Power Administration
- Four CODEF functions detected and blocked cyber attacks targeting substation circuit breakers and intelligent electronic devices
Quantum Encryption Key Distribution Techniques

Quantum Key Distribution Benefits:

• LANL is developing Quantum Security Modules (QSMs) that securely transmit and receive data from grid control devices encrypted with quantum keys

• When an adversary attempts to intercept an encryption key, it causes an unavoidable distortion in the signal that alerts operators

• Recent technology advances reduced the facility footprint and improved the performance:
  o Size of the installed hardware reduced by a factor of five
  o Operating range doubled and increased the key generation rate by 73%

Reduced Footprint of Quantum Communication System

Los Alamos National Laboratory
EST. 1943
Developing Strategic Cybersecurity Core Capabilities at DOE National Laboratories

<table>
<thead>
<tr>
<th>National Laboratory</th>
<th>CEDS R&amp;D Strategic Core Capability Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANL</td>
<td>Power system applications that are cyber-aware</td>
</tr>
<tr>
<td>BNL</td>
<td>Cybersecurity for energy sector forecasting data</td>
</tr>
<tr>
<td>INL</td>
<td>Cyber-informed development and engineering for next generation resilient energy delivery systems.</td>
</tr>
<tr>
<td>LANL</td>
<td>Quantum Key Distribution (QKD) for the energy sector</td>
</tr>
<tr>
<td>LBNL</td>
<td>Detecting cyber incidents in the distribution-level grid</td>
</tr>
<tr>
<td>LLNL</td>
<td>Reliable active mapping for operational networks</td>
</tr>
<tr>
<td>ORNL</td>
<td>Detecting adversarial presence in energy delivery control systems</td>
</tr>
<tr>
<td>PNNL</td>
<td>Enhanced situational awareness using federated power system data</td>
</tr>
<tr>
<td>SNL</td>
<td>Energy delivery systems that confront the adversary with a moving target</td>
</tr>
</tbody>
</table>
DOE Awards for Next Generation Cybersecurity Technologies and Tools

DOE awarded $20 million for 20 new projects to

- Support critical early stage R&D of next-generation tools and technologies
- Build capacity throughout the energy sector for day-to-day operations such as cyber-threat information sharing

<table>
<thead>
<tr>
<th>DOE Technology Focus</th>
<th>DOE Technology Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-Generation Attack-Resilient Electricity Distribution Systems</td>
<td>Energy Delivery Systems with Verifiable Trustworthiness</td>
</tr>
<tr>
<td>(FIT) Firmware Indicator Translation</td>
<td>Malware Operational Mitigation (MOM)</td>
</tr>
<tr>
<td>Adaptive Control of Electric Grid Components for Cyber-Resiliency</td>
<td>KISS (Keyless Infrastructure Security Solution)</td>
</tr>
<tr>
<td>Cyber Interconnection Analysis for High Penetration of DER</td>
<td>MEEDS (Mitigation of External-exposure of Energy Delivery System Equipment)</td>
</tr>
<tr>
<td>GPS Interference Detection</td>
<td>SASS-E (Safe &amp; Secure Autonomous Scanning Solution for Energy Delivery Systems)</td>
</tr>
<tr>
<td>Secure SCADA Protocol Characterization and Standardization</td>
<td>SDN4EDS (Software Defined Networking for Energy Delivery Systems)</td>
</tr>
<tr>
<td>Quantum Key Distribution for the Energy Sector: Trusted Node Relays and Networks</td>
<td>UUDEX (Universal Utility Data Exchange)</td>
</tr>
<tr>
<td>(Module-OT) Modular Security Apparatus for Managing Distributed Cryptography for Command &amp; Control Messages on Operational Technology (OT) Networks</td>
<td>VERITAS (Vulnerability, Exploit, and Risk Identification Toolset and Source)</td>
</tr>
<tr>
<td>DarkNet</td>
<td>Containerized Application Security for Industrial Control Systems</td>
</tr>
<tr>
<td>Quantum Physics Secured Communications for the Energy Sector</td>
<td>Survivable ICS</td>
</tr>
</tbody>
</table>
THE END
Today’s Energy Delivery Systems: More Complex with an Increasing Attack Surface

**Operational Technology (OT) Environment**
Controls physical energy delivery processes

**Information Technology (IT) Environment**
Includes Internet-connected business networks
Managing Cyber Risks Must Be a Shared Responsibility

Security Roles and Responsibilities for Physical and Cyber Risks

Physical Risks

Fed Govt. ↓ Private Sector

- Nuclear Attack
  - Natural Disasters
  - Active Shooter
  - Insider Threats
  - Accidents
  - Theft and Vandalism

Cyber Risks

Fed Govt. ↑ Private Sector

- Nation-State Attack
  - Terrorists
  - Organized Crime
  - Hacktivists
  - Script Kiddies
  - Accidents

Source: NIAC Cyber Scoping Study, February 2017