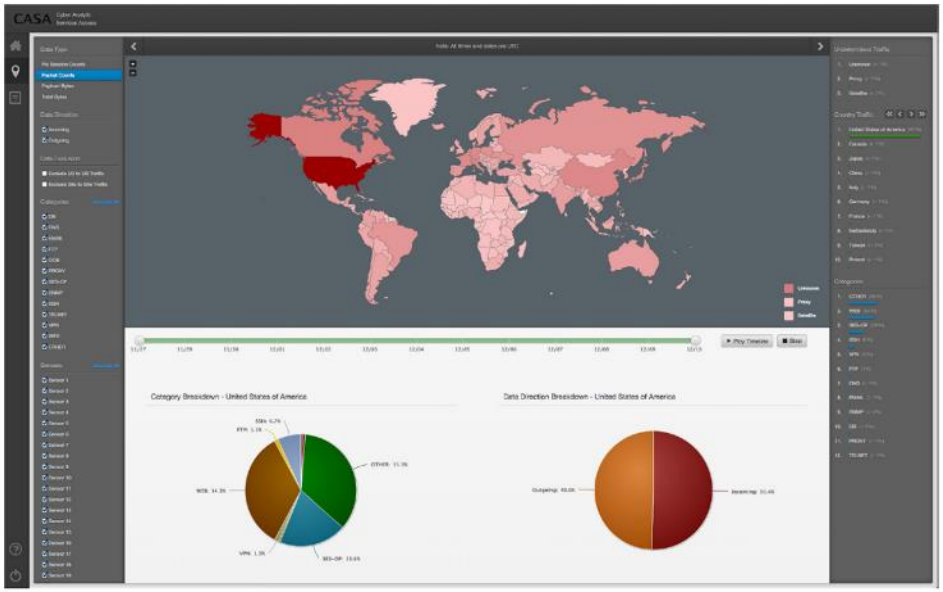
Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Improving the Cyber Resilience of the U.S. Electric Power System

Carl Imhoff
PNNL Electricity Infrastructure Sector Lead
Grid Modernization Lab Consortium Chair

Discussion Topics

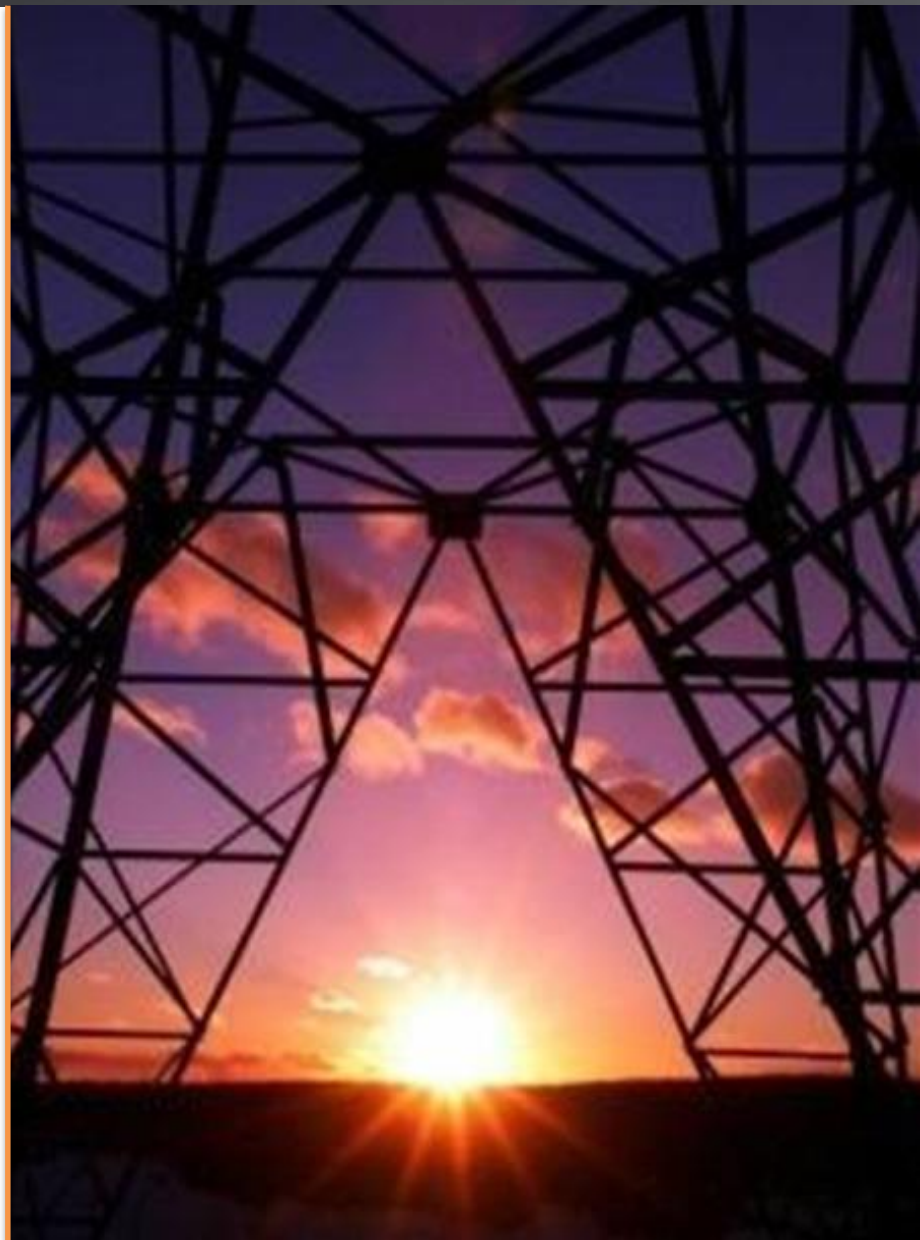
- View of national power system cyber resilience status and DOE engagements (baseline)
- Introduce Lab views of near-term opportunities to improve grid cyber resilience
- Frame emerging fundamental opportunities to advance cyber resilience
- Suggested key questions



Grid Cyber Resilience- Challenge

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

- Traditional grid increasingly reliant on digital components/ communications.
- Internet economy increasingly pervasive at grid edge.
- U.S. grid under constant probing, attack.
- Industry has responded significantly, gaps remain.



Why DOE?

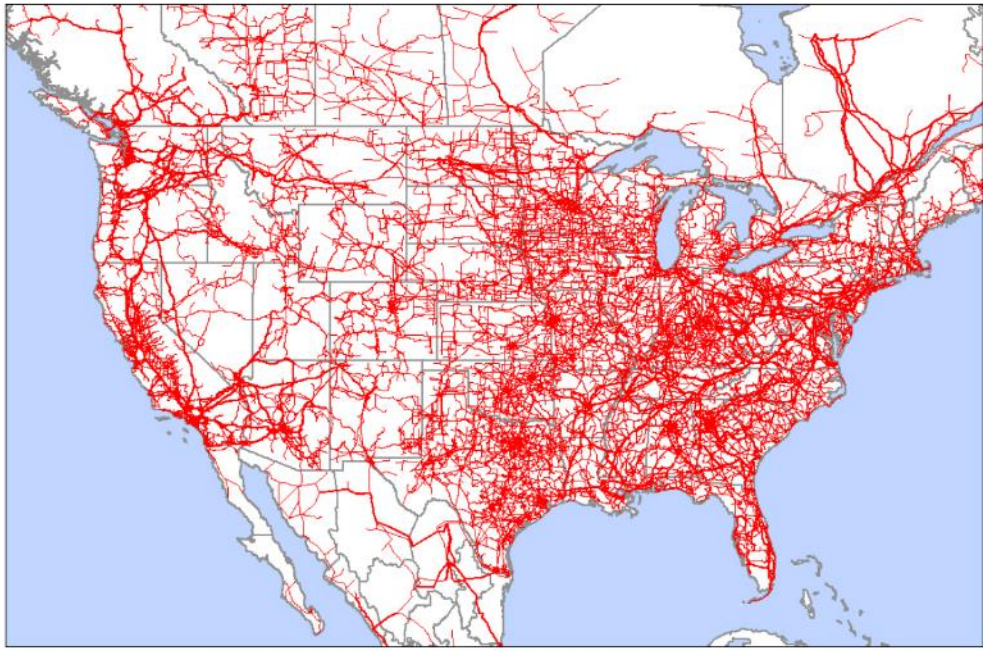
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- 2015 FAST Act:
  - Assigned DOE as lead sector-specific agency for cyber security for energy sector.
  - Gave Secretary of Energy authority to address grid-related emergencies caused by cyber-attacks and physical attacks.
- DOE/national labs uniquely engaged at nexus of classified intelligence and non-classified utility operational awareness.
- Steward for fundamental science and applied power system and “connected assets” R&D

National Perspective

U.S. electric power system vulnerable as result of:

- Incomplete implementation of cyber-security best practices
- Limited access to near-real-time situational awareness and information sharing of cyber-threats and vulnerabilities
- Growing use of digital systems and public internet
- Increasing sophistication of threat actors, both foreign and domestic.



National Cyber Innovation Landscape

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Utilities securing communications and IT business systems
  - North American Electric Reliability Corp. standards
  - Executive collaboration across public and private utilities.
- Vendors innovating proprietary IT solutions, cyber tools.
- Lab system conducting fundamental research/specialized testing and support; leading transition to control systems protection
  - SNL – encryption
  - ORNL – alternate communication
  - INL – control system, wireless communications
  - PNNL – grid cyber intel info sharing, response exercise development, and situational awareness and recovery
  - LANL – Quantum Key encryption.
- University partnerships linking fundamental research and workforce development
  - Cyber Resilient Energy Delivery Consortium (U of Illinois)
  - Cybersecurity Center for Secure Evolvable Energy Delivery Systems (U of Arkansas).
  - Numerous additional niche academic collaborations

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

SEEDS
CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

DOE Efforts linked to Cyber Resilience

- **OE Cyber Security for Energy Delivery Systems (CEDS) Program**
  - **Ongoing research; Lab Call announcements this week**
  - **Revised MYPP undergoing external review and comment**

- OE Advanced Grid Modeling Program extending new high performance dynamic contingency modeling framework
- ARPAE
  - Distributed controls frameworks for resilience to all hazards
  - Data and modeling repositories to accelerate innovation ecosystem
- Office of Science
  - Math Centers working theory underlying advanced control
  - First grid application in exascale computing program emerging
- EERE end-use programs initiating direct efforts relating to “IOT” best practice.
- OCIO cyber initiatives

DOE Outreach and Response

- Supporting Incident Response (Steady State and Crisis State)
- Supporting Information Sharing and Situational Awareness
- Supporting Cyber Exercises
- Supporting maturity model self-assessments (C2M2)
- Supporting Sector Engagements

DOE Grid Modernization Highlights

- Foundational efforts in **grid metrics and valuation tools** – key to systematic regulatory treatment of resilience to cyber /"all hazards"

- **Grid architecture** framing reference views of changing roles of communications systems, controls systems, markets, fuel supply etc..
  - Illuminates changes in grid elements key to cyber resilience
  - Examining alternate approaches to delivering communications resources
  - Considering emerging market concepts (e.g. DSOs, blockchain etc.)

- Roadmaps for **sensing and system observability** in "modern grid".
  - Sensing roadmaps
  - Data analytics

- Advanced **controls and predictive real-time tools**

- **Resilient Distribution Lab Call** awards from OE and EERE

National Labs Develop White Paper on Improving Grid-Cyber

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

1. Rapidly implement preventative cyber best practices for vulnerable mid-sized utilities.

2. Dramatically improve near-real-time cyber-situational awareness and information sharing.

3. Secure U.S. electric power system infrastructure life-cycle integrity.

4. Deliver fundamental R&D to securing electric power system against evolving threats.

INL Idaho National Laboratory

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Sandia National Laboratories

OAK RIDGE National Laboratory

Expected Outcomes

1. Cyber best practices implemented across all utilities.

2. DOE supports near-real time cyber situational awareness linked to intel community. Broaden coverage to mid-size utilities, increase speed and affordability

3. Uniform best practices, standards, and certification deployed for next-generation hardware, software, and control systems.

4. Fundamental research base focused on vulnerability- and consequence-based tools and techniques.

Where Can Collective Efforts Have Biggest Impact?

- **Large utilities** (>50,000 customers):
  - Responded to emerging cyber-threats with cyber self-assessments, best practices, information sharing.
- **Mid-size utilities** (5,000-50,000 customers):
  - Lack expertise, resources to consistently implement and maintain best practices in electric power system cyber security.
- **Small utilities** (<5,000 customers):
  - Have minimal risk of outage from cyber-attack due to simple power systems and limited number of vulnerable modern digital systems.

Mid-size utility of 5,000 – 50,000 customer range.

Securing Grid System Component Supply Chain

- Product development
  - Requirements
  - Design
  - Test
- Acquisition
  - Requirements & procurement language
  - Testing
  - Installation
- Maintenance
  - Patching
  - Upgrades
  - Critical component certification
- Retirement
  - Removal
  - Destruction

Emerging Fundamental Research Topics

1. Addressing operational / control technology cyber resilience (OT)
2. Integrated situational awareness across information technology (IT) and OT
3. Advanced mathematics and algorithms for distributed control and adaptive control
4. System protection theory alternatives under emerging distributed grid models
5. Modeling and simulation of extraordinarily large data sets
6. Application of deep learning to grid data sets and automated machine-to-machine tools
7. Supply chain risk characterization
8. Novel system authentication and management methods
9. Alternative communications network concepts
10. New fundamental grid elements: storage + power electronics+ distributed control theory

Machine Learning for Advanced Analytics

- Data volumes of too large and diverse to manage without novel methods
- Data sets are robust enough that machine learning algorithms can be applied to generate increased automated reporting and “smarter data analysis”
- Value propositions to grid
  - Automated anomaly detection in OT operations to indicate intrusion
  - Data synthesis across IT and OT systems for complete system “health” picture
  - Move from reactive analytics to proactive and predictive analytics

Closing Thoughts for Consideration

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

KEY QUESTIONS

- Is cyber resilience primarily a public goods issue with strong federal role?
- How to rapidly ensure “good hygiene” across nation’s power system?
- How to continually improve defenses (OT,IT and OT+IT) systems?
- How to better prepare for and respond to incidents?
- How to design AND TRANSITION TO an inherently resilient, flexible future system?

SCIENCE AND TECHNOLOGY OPPORTUNITIES

- High performance computing for real-time predictive operations, high fidelity planning, and anomaly/intrusion detection (analytics)
- Deep learning for grid data analytics
- Advanced grid architectures for “all hazards”; informs theory for control, protection and recovery
- Valuation tools for cyber resilience to guide investment


Mission
We transform the world through courageous discovery and innovation.
Vision
PNNL science and technology inspires and enables the world to live prosperously, safely and securely.
DISCOVERY in Action
Values
CREATIVITY
courage
integrity
Impact
COLLABORATION
Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965