IEEE-Northwest Energy Systems Symposium (NWESS)

Paul Skare
Energy & Environment Directorate
Cybersecurity Program Manager

Philip Craig Jr
National Security Directorate
Sr. Cyber Research Engineer

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

The Pacific Northwest National Laboratory is a DOE Office of Science laboratory in Richland, WA. Operated since 1965 by Battelle, a global non-profit research and development organization committed to science and technology for the greater good.

Mission: Transform the world through courageous discovery and innovation.

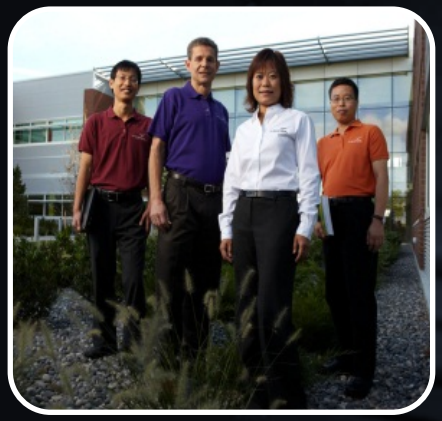
Vision: PNNL science and technology inspires and enables the world to live prosperously, safely, and securely.

Values: Integrity, creativity, collaboration, impact and courage provide the foundation for all we do.

PNNL employs nearly 5,000 staff and has an annual operating budget of $1.1 billion. PNNL has over 100 people working in Electric Infrastructure – over 50 Power System Engineers.

Pacific Northwest
NATIONAL LABORATORY

PNNL draws upon core capabilities, facilities, and investments in Electric Infrastructure



Staff Capabilities

- Power system operation, planning and security
- Power markets
- Demand response
- Renewable integration
- Advanced analytic methods, HPC-based simulations, visualization

Physical Control Center (EIOC)

- Live PMU data from all three interconnections
- PMU data archive
- PowerNET lab
- EMS/DMS displays
- T&D-level data displays
- Platform for tool evaluation, operator training

Cyber Security / Resilience Center (EICC)

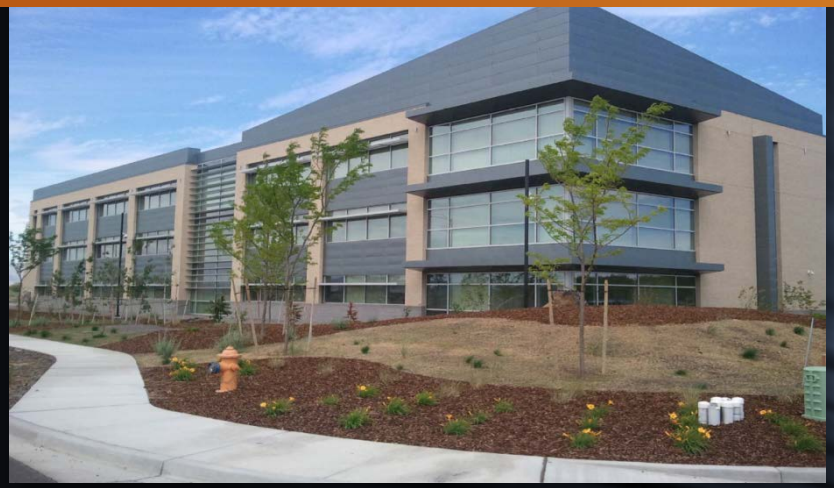
- Live security data streams
- Visual analytics
- Co-located with classified assets that accelerate threat recognition and appropriate response
- Emergency Response
- Public / Private

Future Power Grid Initiative

- Networking and data management
- Advanced analytic methods and HPC approaches for real-time modeling and simulation
- Visualization and decision support
- Next Generation EMS
- Next Generation Simulation

PNNL facilities and unique technologies accelerate innovation and impact

Our strength is derived from applying R&D results to support operational missions



Systems Engineering Facility

Cyber Innovation & Operations Center

Computational Sciences Facility

Electricity Information & Operations Center

Abstract

From business needs, to initial planning, procurement, receiving, deployment, operation, maintenance, to retirement, an overview of the entire control system lifecycle, and how cyber security fits into each phase. Compliance has improved many aspects of our nation electric utility cyber security posture, but what about where compliance does not apply?

What resources are there for stakeholders to turn to, like the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), and how can I use them today?

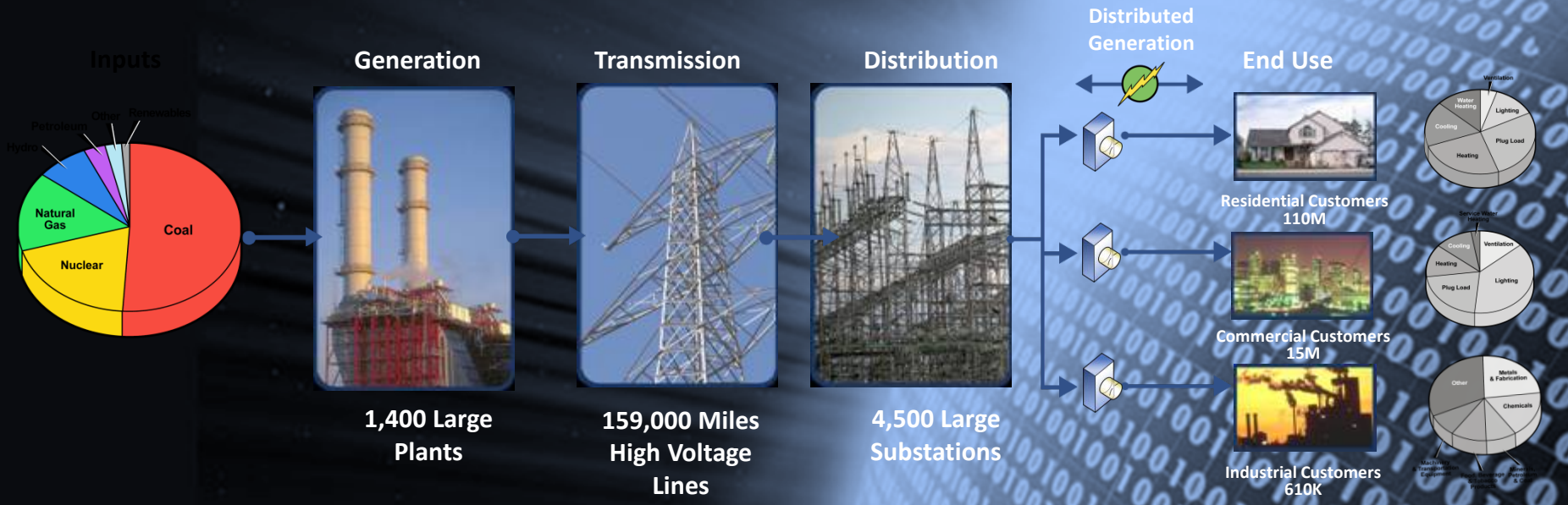
Pacific Northwest
NATIONAL LABORATORY

Control Systems Security

- Vulnerability assessments for SCADA and other control systems
- Unique systems architectures, experimentation, modeling and simulation
- Secure protocols to authenticate communication
- Reverse engineering and specialized equipment
- Partnerships with government and industry

Pacific Northwest
NATIONAL LABORATORY

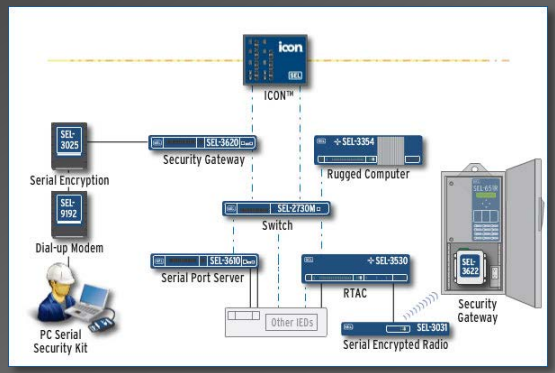
Power: Inventory of U.S. Electrical Infrastructure Assets



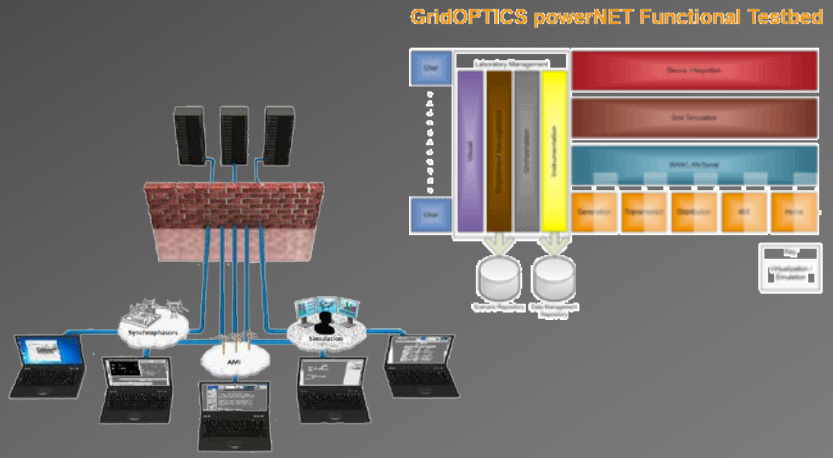
- More than 4,700 generation plants in the U.S.
  - 1,400 are greater than 100 MW **and generate 95% of the electricity**
- More than 350,000 miles of transmission lines in the U.S.
  - 159,000 miles are greater than 230 kV
- More than 21,600 substations in the U.S.
  - 4,500 are larger than 230 kV

CI / KR Control Systems

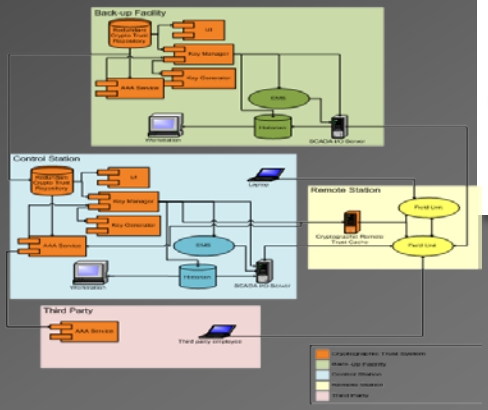
Commercialized Security Technology

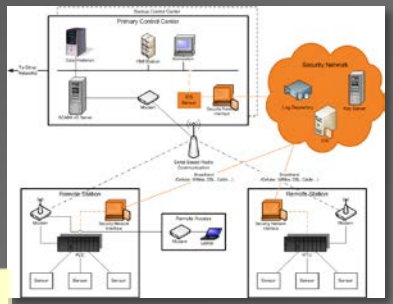


Internal Investments



Trusted Security Paradigms





Next Generation Control System Simulation

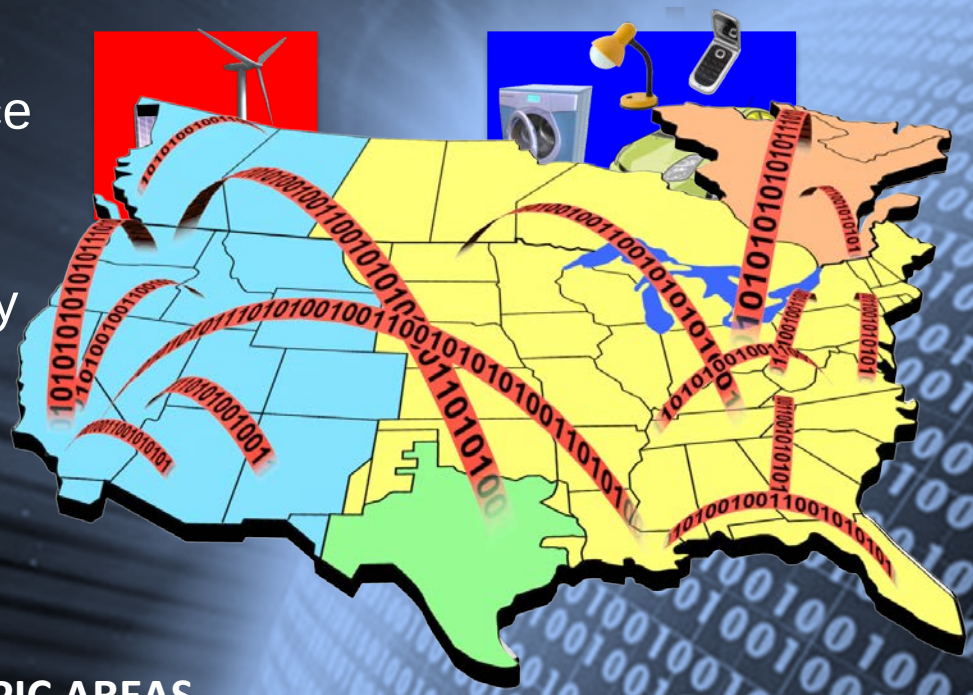
Trends Impacting Control System Security

- **Open Protocols**
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- **General Purpose Computing Equipment and Software**
  - Standardized computational platforms increasingly used to support control system applications
- **Interconnected to Other Systems**
  - Connections with enterprise networks to obtain productivity improvements and information sharing
- **Reliance on External Communications**
  - Increasing use of public telecommunication systems, the Internet, and wireless for control system communications
- **Increased Capability of Field Equipment**
  - "Smart" sensors and controls with enhanced capability and functionality

KEY: COMMUNICATONS/CONNECTIVITY

Power Grid Transformation

- Department of Energy-Office of Emergency Operations-Electricity Delivery and Energy Reliability, Recovery **$3,672,233,727**
- 50% Cost share = Approx**$8B** infrastructure upgrades, improvements, research



SMART GRID INVESTMENT TOPIC AREAS

Equipment Manufacturing
Customer Systems
Advanced Metering Infrastructure
Electric Distribution Systems
Electric Transmission Systems

Integrated and/or Crosscutting Systems

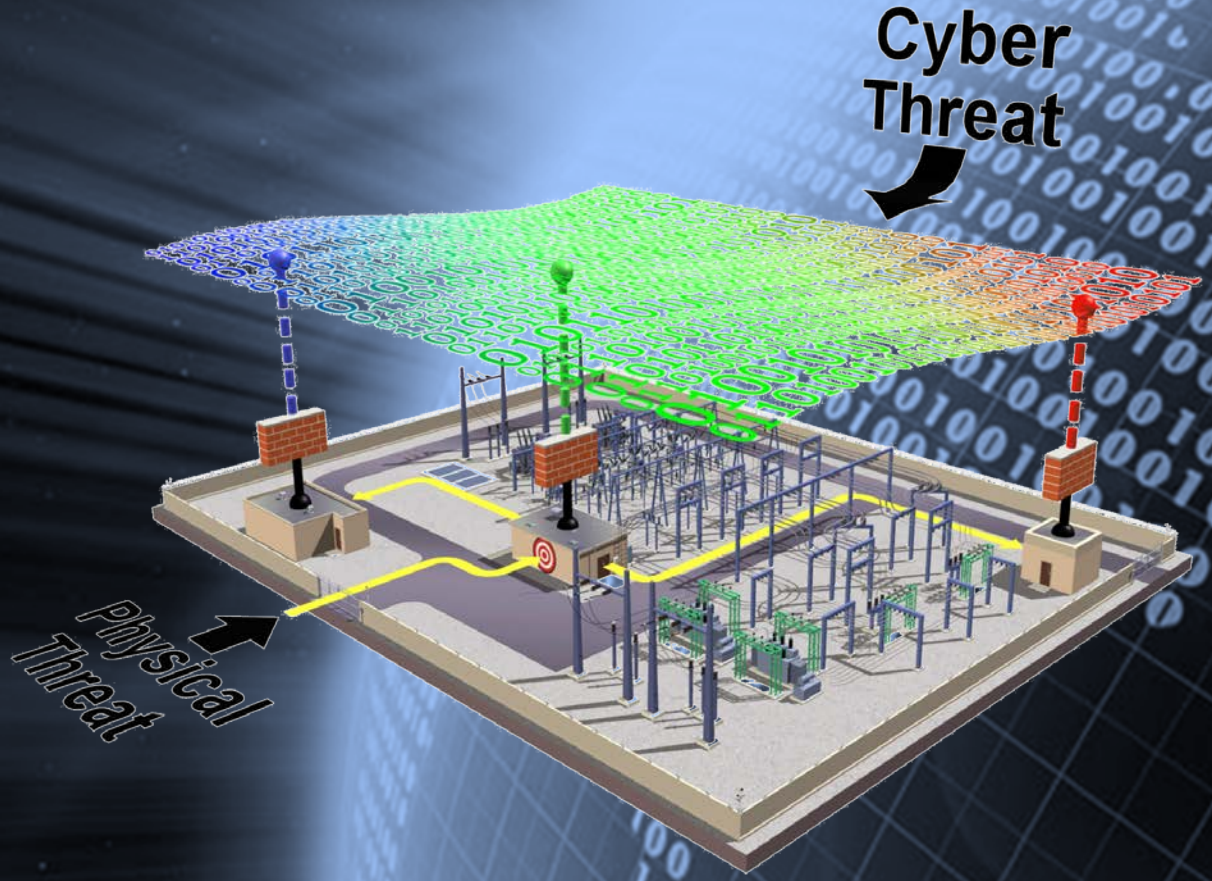
AMERICAN RECOVERY & REINVESTMENT ACT

RECOVERY.GOV

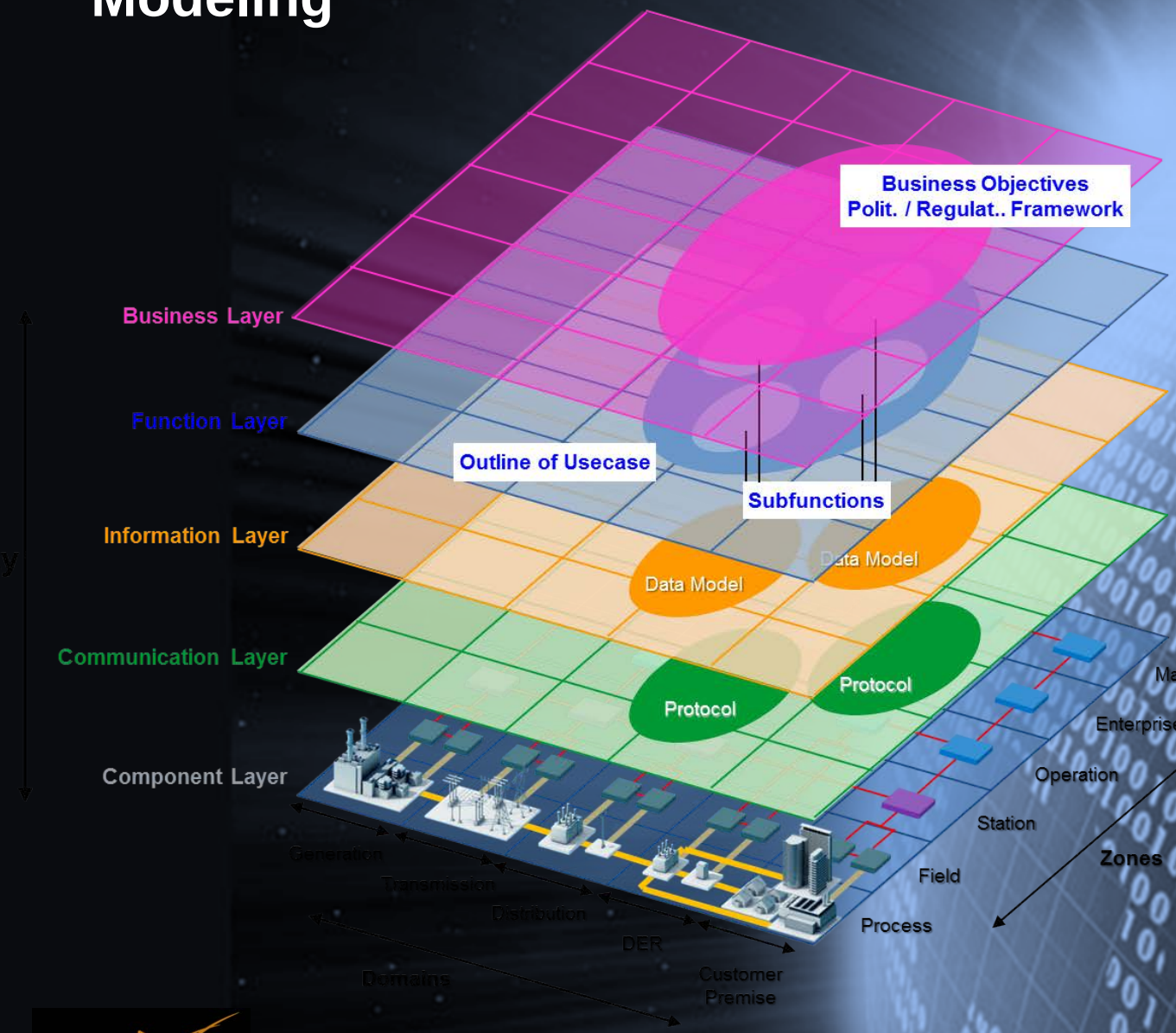
DOE Cyber Mission for ARRA

CYBERSECURITY

- Cyber/Physical
- Security Controls
- Cybersecurity plan
- Scale
- Impacts to projects
- Sustainable



Alignment with emerging Smart Grid Architecture Modeling



Pacific Northwest
NATIONAL LABORATORY

Basics: What You Need To Know About The Electric Utility Organizational Processes

Risk Management (Analyze Risk)

Asset Configuration Management (Inventory, Architecture, Software Upgrades

Identity and Access Management (Role Based Access for Application and Physical Access)

Threat and Vulnerability Management (New IT, OT Technologies)

Situational Awareness (Monitoring / Intrusion Detection Tools)

Information Sharing and Communications

Event and Incident Response (Detect and Respond)

Supply Chain and External Dependencies Management

Workforce Management

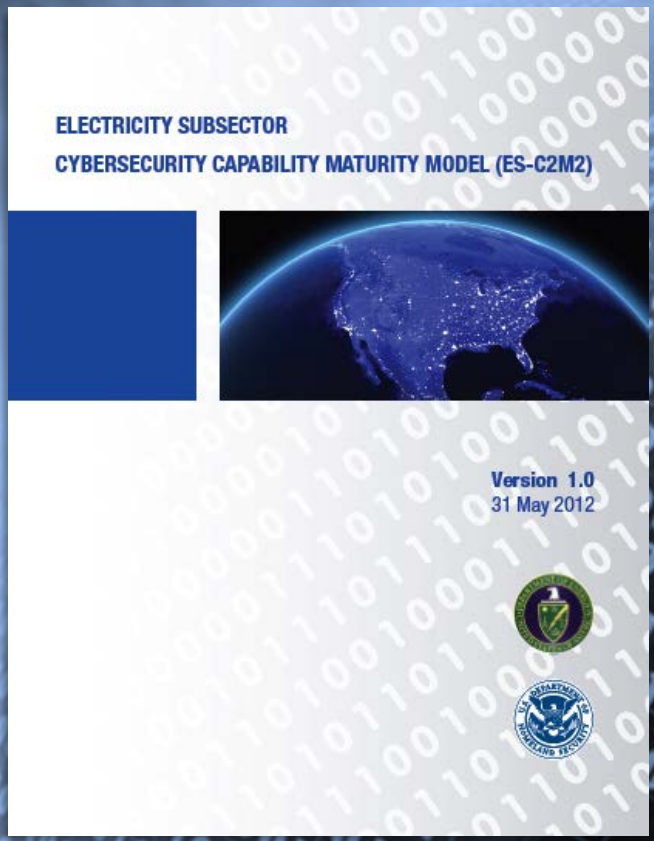
10 Domains: Logical groupings of cybersecurity goals

Utility Resources: How To Get There

RISK	DOE RMP, NIST SP800-30, NRECA Guide to Developing a Cyber Security & Risk Mitigation Plan, ISO 27005:2011, SCADA AU RMF
ASSET	ISO/IEC 27002:2005, NISTIR 7628 Vol. 1, NERC CIP-002
ACCESS	NISTIR 7628 Vol 1., NERC CIP-002/004/005/007, NIST SP800-53
THREAT	NIST SP800-40, NERC ES-ISAC, DHS ICS-CERT, CRISP, NVE, Vendors, NERC CIP-005/007
SITUATION	NIST SP800-137, NRECA Guide to Developing a Cyber Security & Risk Mitigation Plan, NERC RTSA
SHARING	NERC Security Guideline: Information Protection, NERC ES-ISAC, FERC CEII, DHS PCII
RESPONSE	NSIT SP800-40/61/82/83/86, NERC ES-ISAC, DHS ICS-CERT, NERC GridEx
DEPENDENCIES	DOE OE Cybersecurity Procurement Language for Energy Delivery Systems, NRECA Security Questions for Vendors, NISTIR 7622, MIT SCMM, ISO 28001:2007, Filsinger 2012
WORKFORCE	NERC CIP-004, CERT RMM, PM/HRM/OTA, NIST SP800-16/35/50/53/82, DOE OE Secure Power Systems Professional (SPSP), NERC GridEx
CYBER	NERC CIP-001/002/003/004/005/006/007/008/009, NIST SP800-35/53/64/82

Measuring the Maturity of Cybersecurity Capability

- ES-Cybersecurity Maturity Model (ES-C2M2)
  - Support ongoing development and measurement of cybersecurity capabilities within the electricity subsector through the following four objectives:
    - Strengthen cybersecurity capabilities in the electricity subsector
    - Enable utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities
    - Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities
    - Enable utilities to prioritize actions and investments to improve cybersecurity



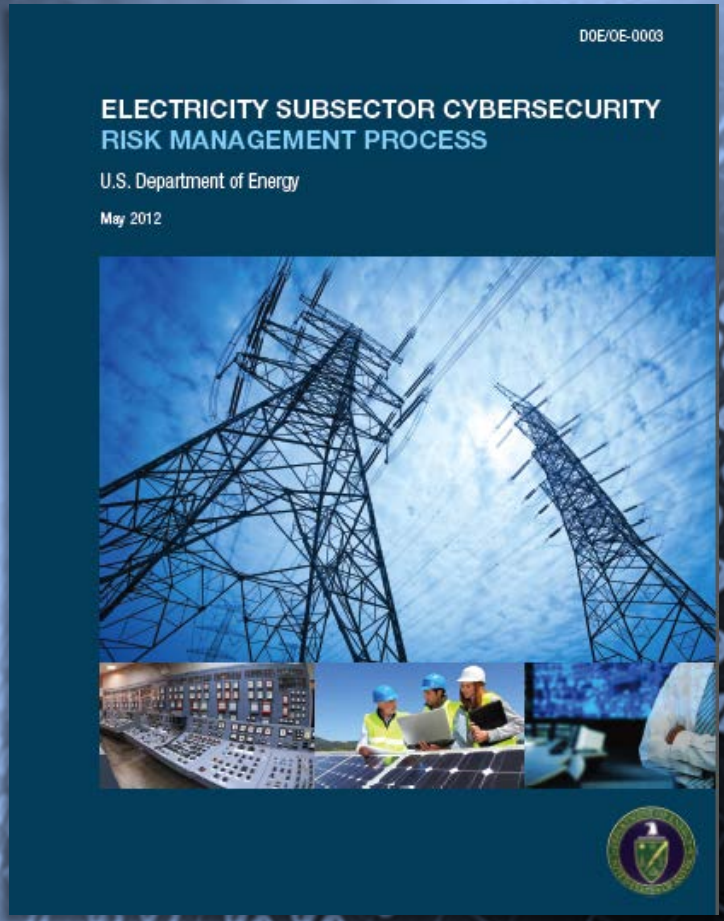
http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program

Basics: What You Need To Know about Risk Management

- Basically, security is Risk Management
- This allows financial investment for security to be targeted where it is needed most
- Considerations:
  - Threats
  - Vulnerabilities
  - Impacts
    - **Risk = Threats x Vulnerabilities x Impact**
- Return on Investment has been a long standing ‘holy grail’
  - Logging events to show possible attacks is one of the approaches to show ROI

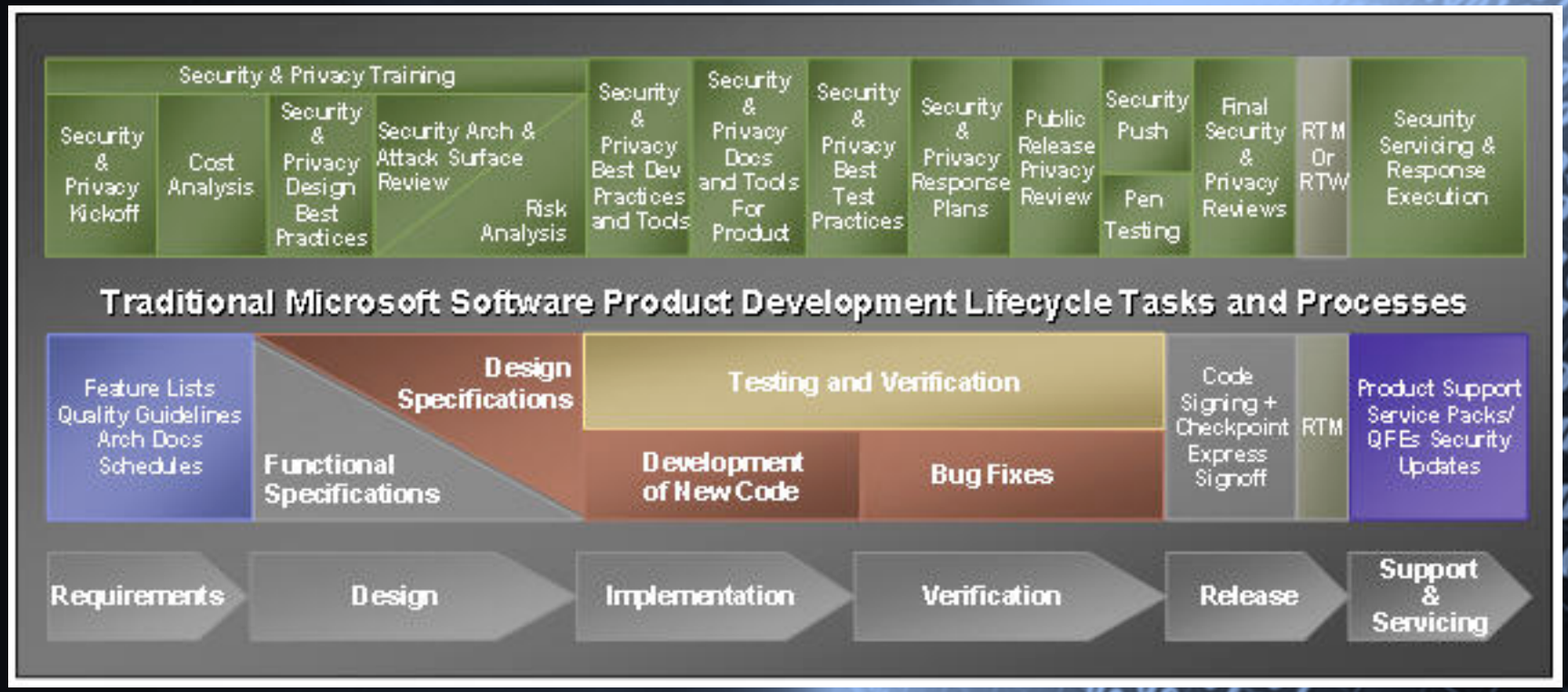
Tools to get there: Risk Management Process

- Risk Management Process
  - The electricity subsector cybersecurity Risk Management Process (RMP) guideline has been developed by a team of government and industry representatives to provide a consistent and repeatable approach to managing cybersecurity risk across the electricity subsector



http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program

Basics: What You Need To Know About Software Development Lifecycle Secure Coding Guidelines must be pervasive



http://www.corporatewebbing.com/sdl/sdl.jpg

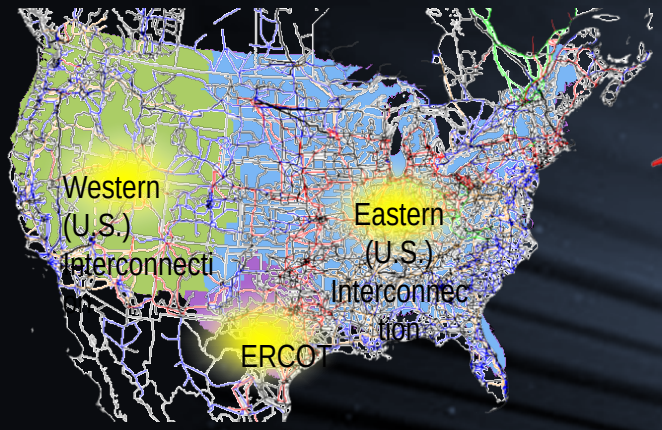
Utility Resources: How to Get There

www.cert.org/secure-coding

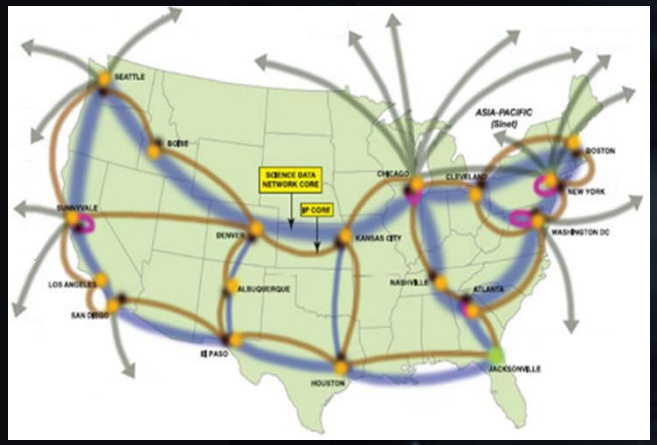
The CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems, Second Edition
Java Coding Guidelines
CERT Oracle Secure Coding Standard for Java
Supporting the Use of CERT Secure Coding Standards in DoD Acquisitions
Source Code Analysis Laboratory (SCALe)
Secure Coding Initiative
Secure Design Patterns

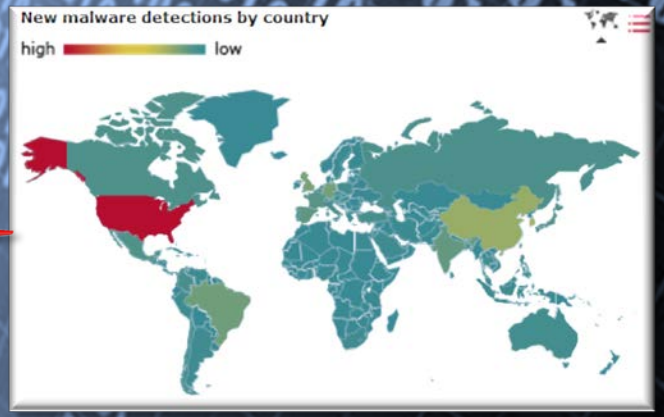
Information Sharing

U.S. Electric Grid /w Smart Sensors



Insider Threat



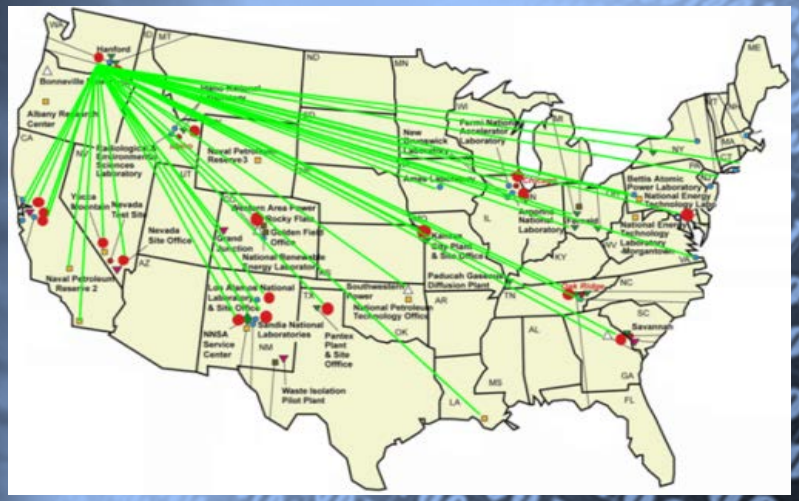


Pacific Northwest
NATIONAL LABORATORY

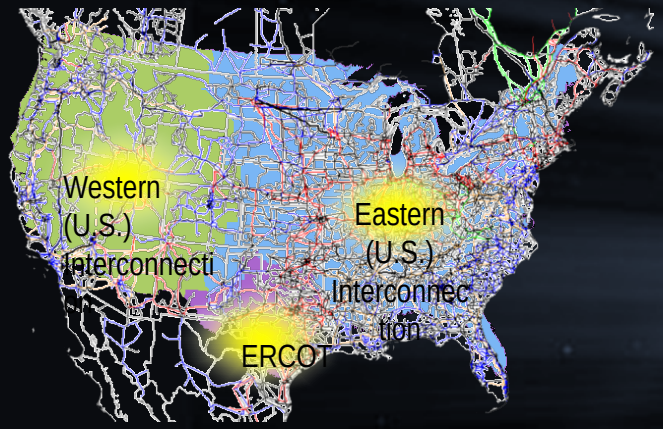
PNNL-210141

Cybersecurity Risk Information Sharing Project (CRISP)

- CRISP builds on the successes of the DOE Cooperative Protection Program (CPP) to deliver an energy sector situational awareness capability for infrastructure protection.



U.S. Electric Grid

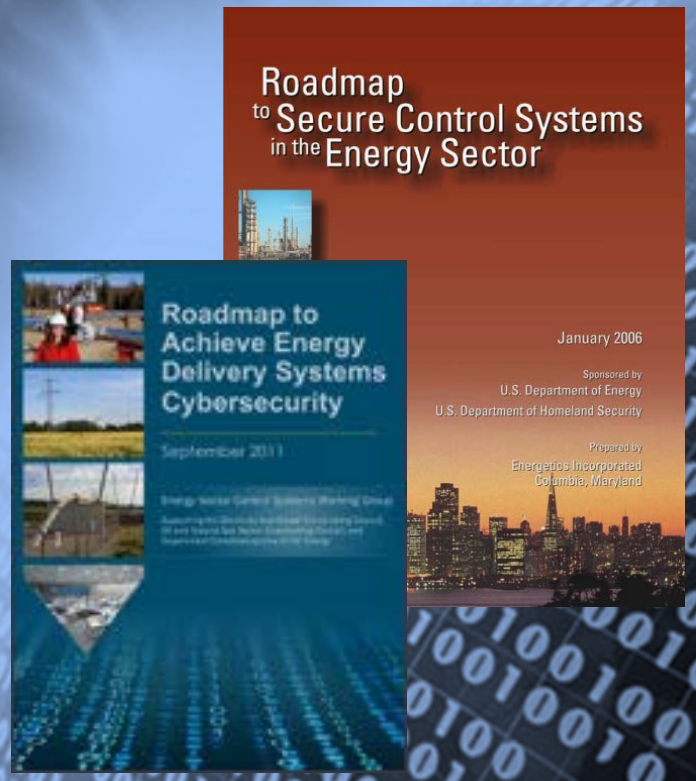


- CRISP is an **industry led** wide-area situational awareness capability enables a real-time operational response to active cyber threats.
- Volunteer sites deploy the technology to provide robust situational awareness tailored to meet the needs of the energy sector.
- Data is shared to gain insights into adversary motives enabling rapid response to emerging threats.

Pacific Northwest
NATIONAL LABORATORY

Strategy: DOE-OE Control Systems Roadmap (R&D)

- CEDS/NSTB (OE10) Research Agenda
- Original Roadmap 2006, updated 2011
  - www.controlsystemsroadmap.net
- Challenges:
  - Address Roadmap with partnered research leading to commercial solutions
  - Influencing Supply Chain
  - ***Advanced Persistent Threat***
    - *Advanced – Operators behind the threat utilize the **full spectrum of intelligence** gathering techniques.*
    - *Persistent – Operators give **priority to a specific task over time**, rather than opportunistically seeking to achieve the defined objectives.*
    - *Threat – Means that operators have a specific objective and are **skilled, motivated, organized and well funded**.*

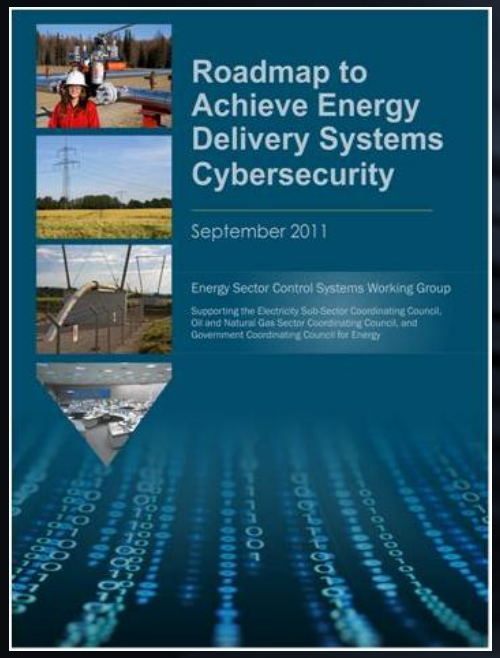


"In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function."

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

Cybersecurity for Energy Delivery Systems (CEDS)

Roadmap – Framework for Collaboration



Energy Sector's synthesis of critical control system 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 control systems security

Roadmap Vision

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

For more information go to: www.controlsystemsroadmap.net

Pacific Northwest NATIONAL LABORATORY

PNNL-210141

National Electric Grid Cyber Exercises

Evolving Goals

- Identify and exercise processes, procedures, relationships, mechanisms that address a cyber incident;
- Examine the role of DHS and its National Cyber Incident Response Plan (NCIRP);
- Assess information sharing issues;
- Examine coordination and decision-making mechanisms; and
- Practically apply elements of ongoing cyber initiatives and findings from past exercises.

GridEx 2011

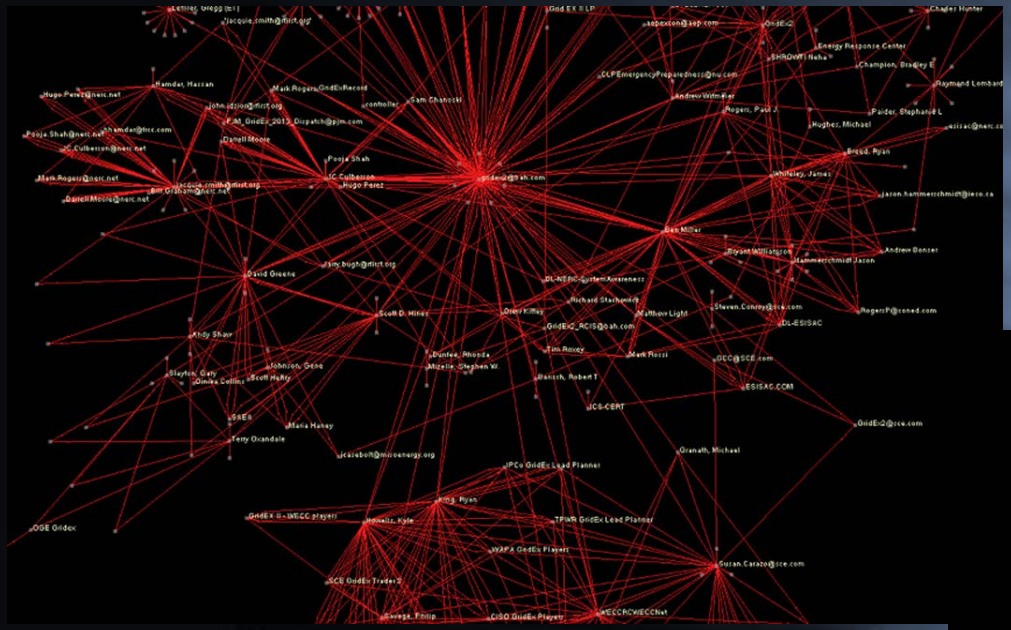
1. Validate the current readiness of the electricity industry to respond to a cyber incident and provide input for security program improvements
2. Exercise NERC and industry crisis response plans and identity gaps in plans, security programs, and skills
3. Assess, test, and validate existing Command, Control and Communication Plans for key NERC stakeholders

GridEx II (2013)

1. Exercise the current readiness of the electricity industry to respond to a security incident, incorporating lessons learned from GridEx 2011
2. Review existing command, control, and communication plans and tools for NERC and its stakeholders
3. Identify potential improvements in physical and cybersecurity plans, programs, and responder skills
4. Explore senior leadership policy decisions and triggers in response to major grid reliability issues

NERC GridEX-II

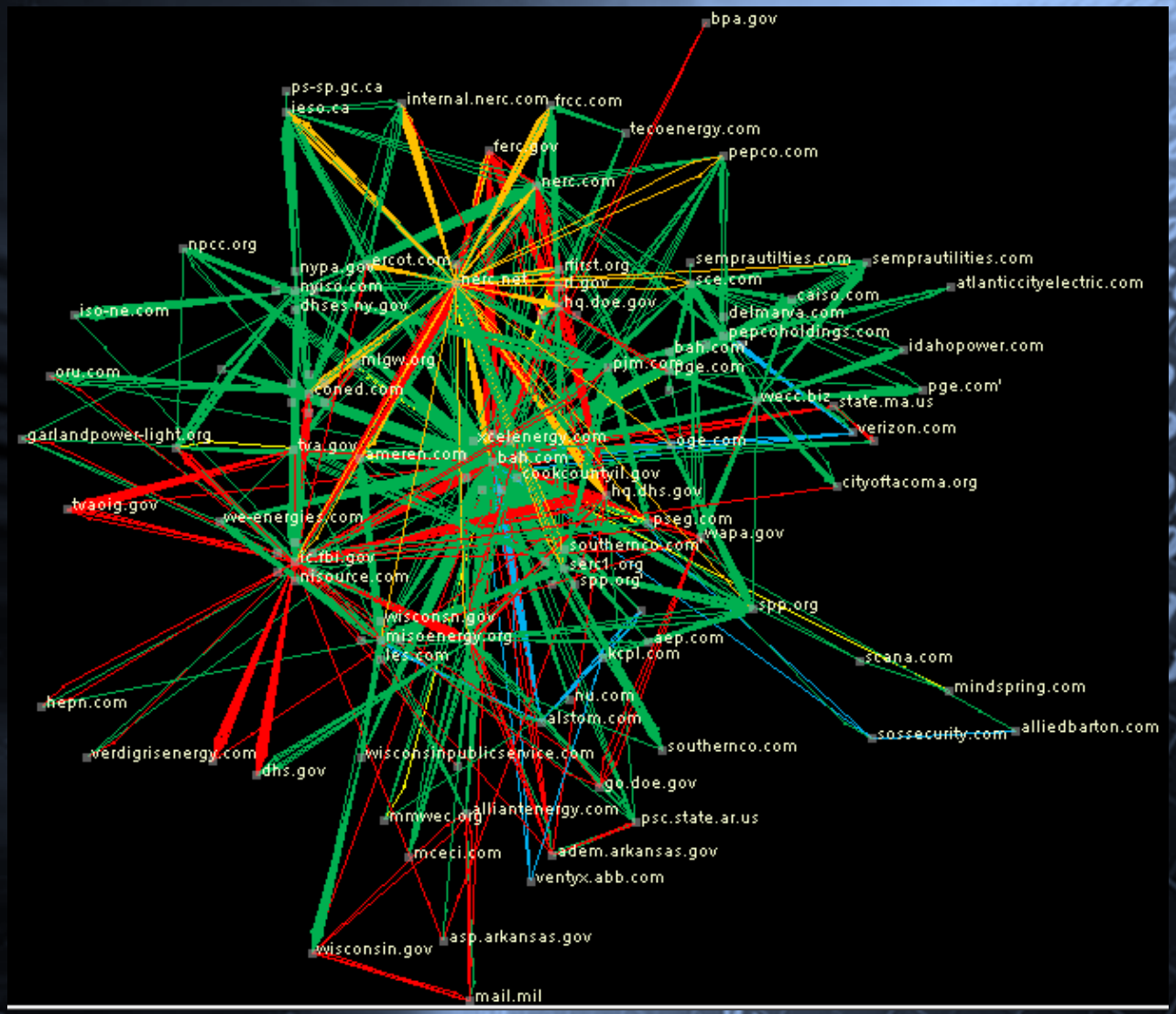
09:30-11:30



11:30–14:40

GridEx-II: Day 1 Summary by Organization

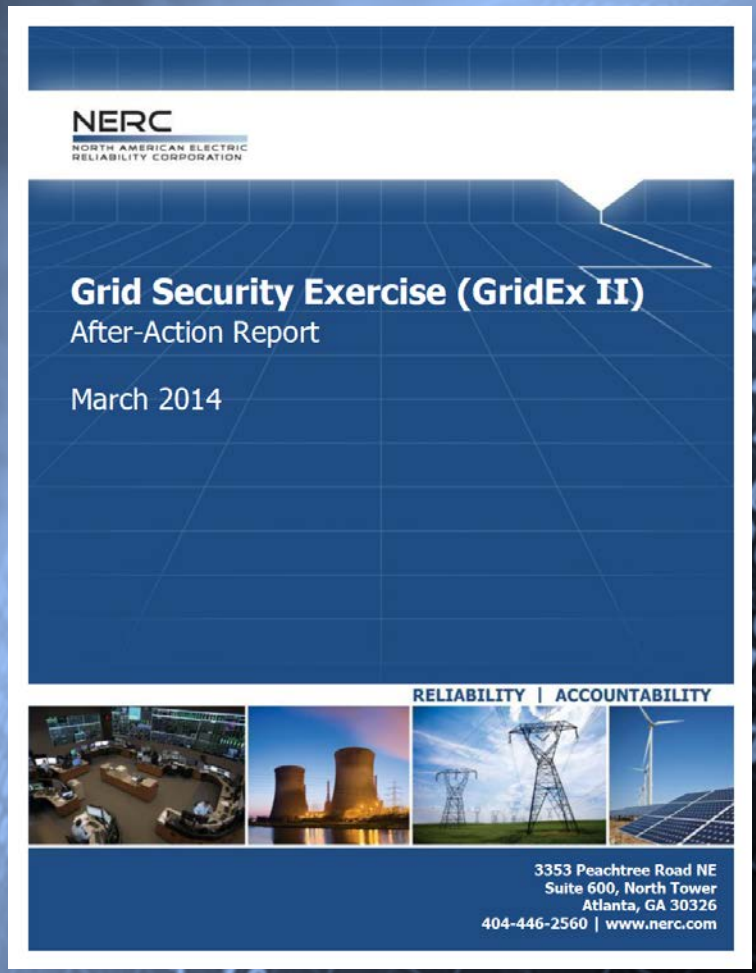
Green – Utility
Orange – Gov
Blue – Vendor
Yellow - NERC



Pacific Northwest NATIONAL LABORATORY

GridEX-II (2014)

- Exercise after-action report
- Grid-Ex I 2011
  - Table Top (Executive)
- Grid-Ex II 2014
  - Highly Expanded to on-site stakeholders
- *Grid-Ex III 2015*
  - *More advanced exercise enabled with structured communications, collaboration*
- *Grid-Ex IV 2017*
  - *Future?*



http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx

Discussion

Paul Skare
Program Manager
Desk 509.372.4210
paul.skare@pnnl.gov

Carl Imhoff
Sector Manager
Desk 509.375-4328
carl.imhoff@pnnl.gov

Dale King
Project Management Office
Desk 509.375.2503
dale.king@pnnl.gov

Phil Craig
Deputy
Desk 509.375-4464
philip.craig@pnnl.gov