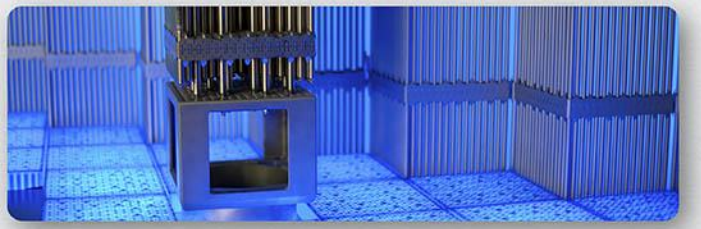


ELECTRIC POWER RESEARCH INSTITUTE

EPRI Cyber Security Projects

NITRD TTS: Solutions for the Smart Grid

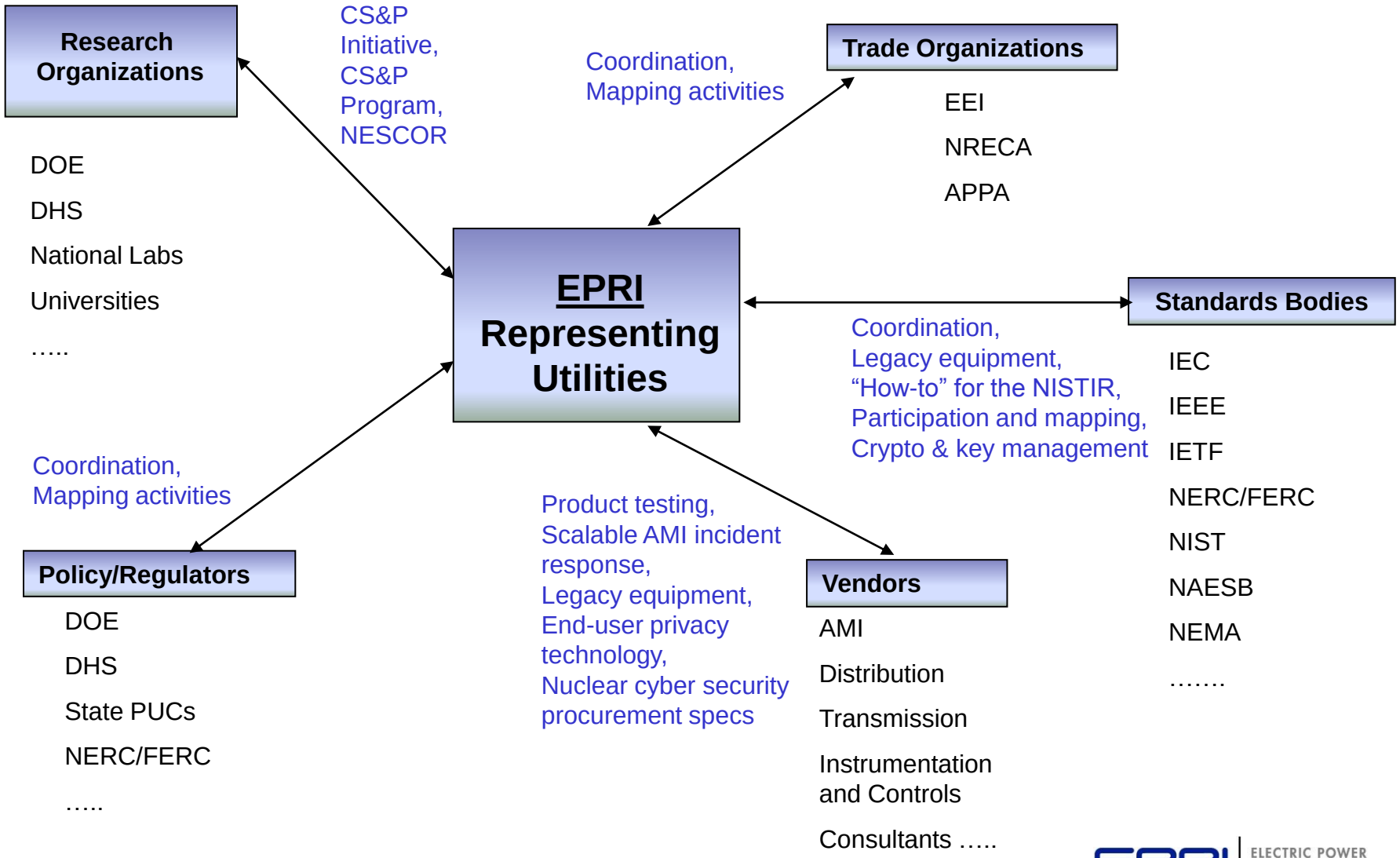
Galen Rasche

Technical Executive

grasche@epri.com

2011-July-20

EPRI Cyber Security Activities Landscape



© 2011 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

DOE National Electric Sector Cyber Security Organization (NESCO)

EnergySec	EPRI
• Primary grant recipient	• Research and analysis
• Information and resource sharing • Collaboration • Situational/tactical awareness • Rapid notification • Forensics	• Mitigate risks from imminent threats and vulnerabilities • Harmonize cyber security requirements • Assess cyber security posture of standards and technologies
• Focus on near-term issues	• Focus on longer-term issues • Support near-term efforts of EnergySec

© 2011 Electric Power Research Institute, Inc. All rights reserved.

EPRI Power Delivery and Utilization (PDU) Cyber Security and Privacy Initiative

Objectives:

- Prevent cyber incidents by creating requirements, developing guidelines, and addressing legacy systems
- Create framework for responding to AMI incidents
- Inform the development of the research agenda for the **Cyber Security and Privacy Program** for the next three to five years

Activities:

Map Activities Landscape	**Protect Legacy Systems**
Guidelines for NISTIR 7628	**AMI Incident Response**
Contribute to Industry Efforts	**Assess Cyber-Physical Attacks**

© 2011 Electric Power Research Institute, Inc. All rights reserved.

Generation Sector Initiative Project

- Cyber Security Strategies for Instrumentation & Control Systems
- 2011 and 2012 Supplemental

- Tasks:
  - Integrating Data Diodes to Meet Compliance
  - Compliant Integration of Wireless Devices into GEN Environment
  - Change Management Tools and Techniques

© 2011 Electric Power Research Institute, Inc. All rights reserved.

Nuclear Sector Initiative Project

- Cyber Security Procurement Requirements For Plant Digital Systems

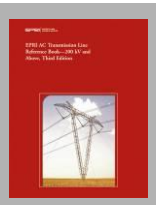
- April 2011 – July 2012 (TBD)

- Scope:
  - Develop generic procurement language for cyber-security requirements
  - Create consensus with utilities and vendors
  - Develop guideline and draft procedures for using the procurement language

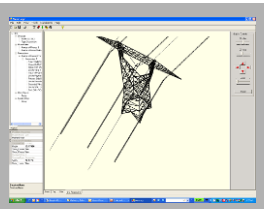
© 2011 Electric Power Research Institute, Inc. All rights reserved.

PDU P183: Cyber Security and Privacy Program Summary Overview

Prevention



Risk Management
For Cyber-Physical Attacks



Security Testing Tools
For End-User Devices

Security Requirements
For New Technology

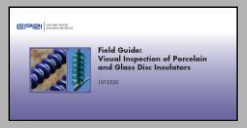
Protection

Secure Remote
Access to Substations

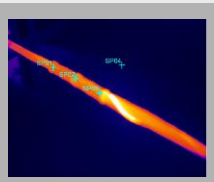
Secure DER
Architectures

Risk Mitigation For
Legacy Systems

Response / Recovery



Standardized AMI
Security Objects



Network and
Security Management
For Transmission

Framework for
Unified Event
Monitoring

Resiliency From
Cyber Incidents

Short Term → Long Term

© 2011 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

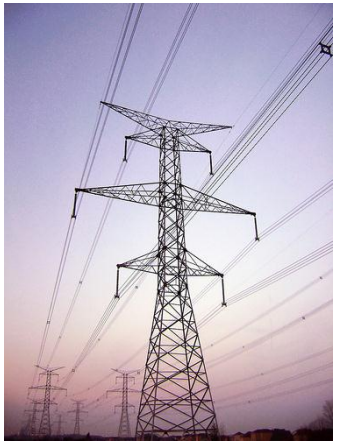
P183A: Cyber Security and Privacy Technology Transfer and Industry Collaboration

- **Mapping the Smart Grid Cyber Security and Privacy Landscape**
  - Provide members regular updates on document
- **Technology Transfer and Industry Collaboration**
  - Support active participation and contribution to:
    - UtiliSec
    - NIST SGIP (CSWG and DPG)
    - NAESB Privacy Task Group
  - Deliver detailed updates on:
    - NERC, DHS ICSJWG
- **White papers on government activities**

© 2011 Electric Power Research Institute, Inc. All rights reserved.

P183B: Security Technology for Transmission and Distribution Systems

- Mitigating risk of legacy equipment
- Frameworks for incident response
- Security Architectures for the Smart Grid



Projects:

- Security Strategies for Legacy Systems
- Network Security Management for Transmission Systems
- Risk Management for Cyber-Physical Incidents
- Assessment of Substation Remote Access Security
- Security Architectures for Distributed Energy Resources

© 2011 Electric Power Research Institute, Inc. All rights reserved.

P183C: Security and Privacy for End Use Technology

- Standardizing AMI security objects

- Supporting user data privacy
  - Scalable key management techniques

Projects:

- Standardized Security Objects for AMI
- Cryptography and Key Management
- Technology Solutions for Supporting Privacy of End-User Data
- Tools and Techniques for Security Testing of End-User Devices

© 2011 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Cryptography and Key Management

- Millions of meters containing crypto keys for:
  - Authentication, integrity of updates and commands, confidentiality
  - Current key management technology does not scale
- Build on work by the CSWG Cryptography Subgroup and the Design Principles Group
- Tasks:
  - Specify primary elements of the Crypto Key Management System (CKMS)
  - Define the performance criteria
  - Select and configure CKMS technology
  - Document the analysis

© 2011 Electric Power Research Institute, Inc. All rights reserved.

Technology for End-User Privacy

- Background
  - Smart Grid enabled bi-directional flow of information
  - Granularity and quantity of information collected
  - Introduction of third-party data access
- Project builds work by CSWG Privacy Subgroup, ABA Privacy Working Group, NAESB Data Privacy Task Force, and the EU Smart Grid Task Force
  - Identify and evaluate technology required to store, aggregate, analyze and protect energy usage
  - Analyze in the context of system bandwidth and processing constraints
  - Develop logical architecture and test a reference implementation

© 2011 Electric Power Research Institute, Inc. All rights reserved.

Discussion

Galen Rasche
grasche@epri.com

© 2011 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

© 2011 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE