

EPRI

ELECTRIC POWER
RESEARCH INSTITUTE

National Electric Sector Cyber Security Organization Resources (NESCOR) Overview

Smart Grid Information Sharing Webcast August 22nd 2011

Erfan Ibrahim

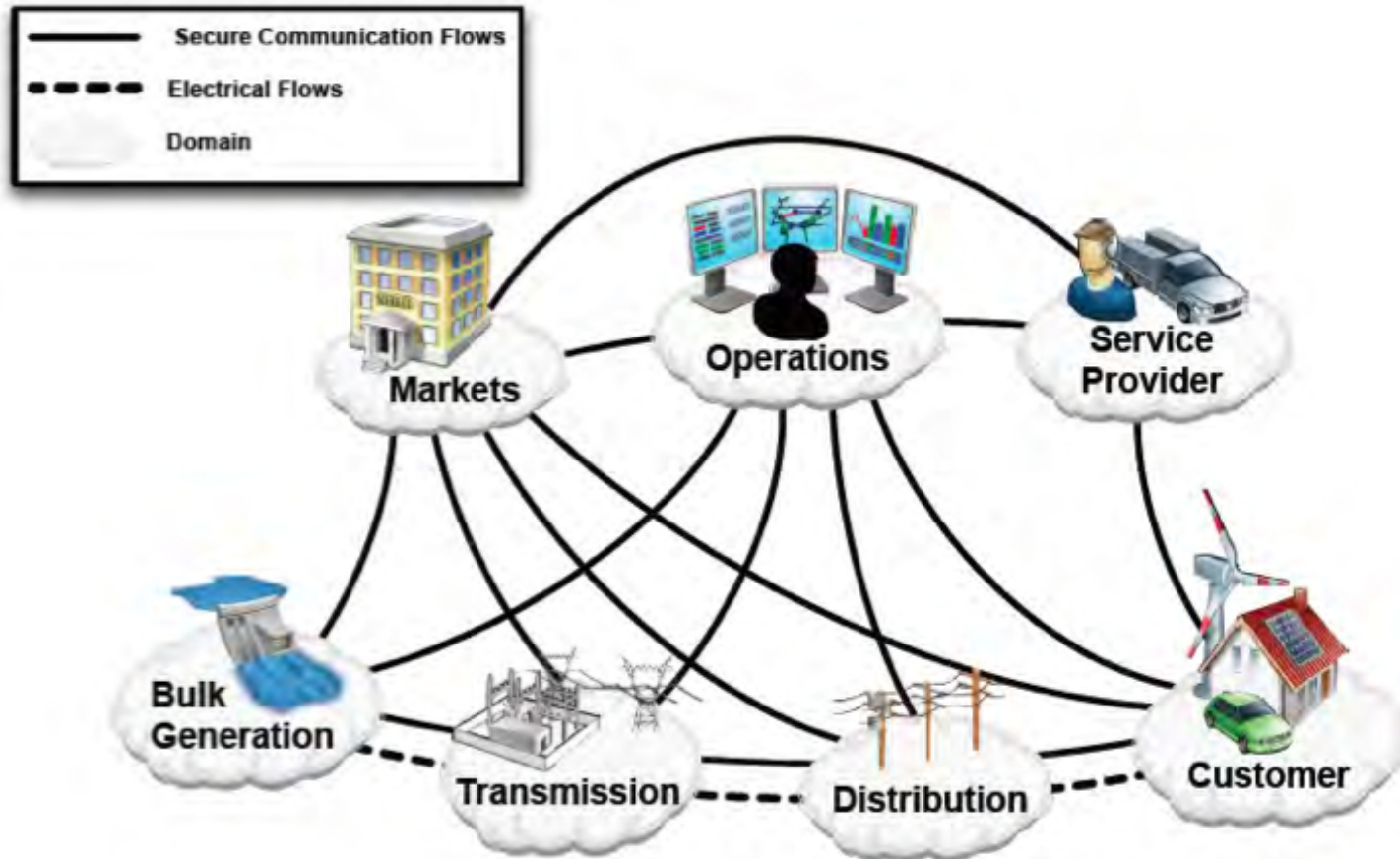
Technical Executive

EPRI NESCOR Lead

Power Delivery and Utilization Sector

EPRI Project Lead

Security Context



Security for the electric sector crosses multiple domains, presenting many new challenges...

NESCO Background

DOE issued a Funding Opportunity Notice (FOA DE 0000245) in April 2010 to establish the National Electric Sector Cyber Security Organization (NESCO) as a public private partnership to:

- Evaluate cyber security posture for legacy systems
- Evaluate deployability of emerging cyber security technologies
- Collaborate and coordinate to identify cyber security requirements
- Perform use case analysis for risk identification, assessment, and development of risk mitigation strategies
- Develop cyber security best practices and metrics
- Establish and operate a Cyber Incident Data Center (CIDC)

• An EPRI Led Team with Support from PDU Executive Committee Members Responded to DOE FOA for NESCO

National Electric Sector Cyber Security Organization (NESCO) Vision

- **Strategic focus:**

- Provide a focal point for bringing together utilities, federal agencies, regulators, and researchers to address the electric sector security threats

- **Program objectives:**

- Develop risk mitigation strategies, best practices and metrics
- Test security technologies in labs and pilot projects
- Harmonize security requirements across bodies of work from DHS, NIST, NERC, etc.
- Assess existing power system and cyber security standards to meet the security requirements of the power system

EPRI Led Team Selected for NESCOR Award

National/ Commercial Research Labs	Academia	Other Subject- Matter Experts
<ul style="list-style-type: none"> • Oak Ridge National Lab • Sandia National Lab • Idaho National Lab • National Renewable Energy Laboratory • Palo Alto Research Center • SRI • Telcordia 	<ul style="list-style-type: none"> • University of Houston • UCLA • UC Berkeley 	<ul style="list-style-type: none"> • N-Dimension • InGuardians • Arc Technical • EnerNex • Xanthus Consulting International • TLI Inc (Texas A&M University) • Adventium Labs (University of Minnesota Smart Grid Consortium)

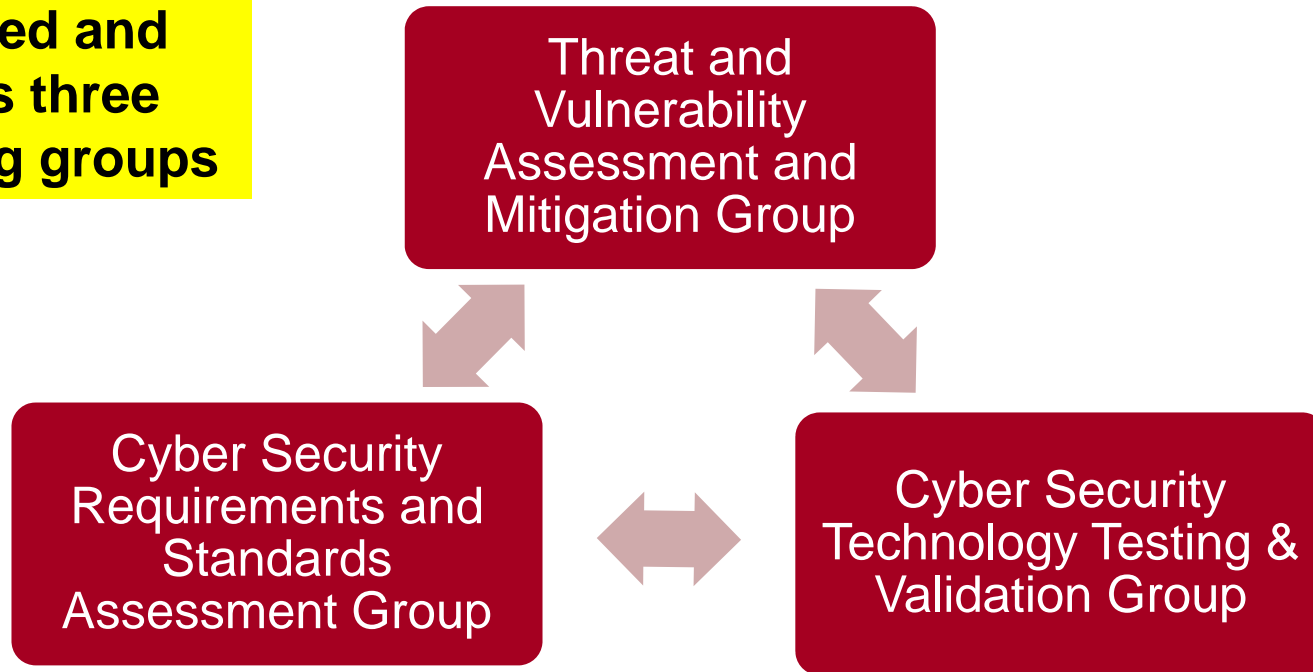
Focus Areas

- Review NIST, NERC and other cyber security requirements and results.
- Assess existing power system and cyber security standards to meet the security requirements of the power system
- Develop failure scenarios, identify vulnerabilities, develop risk mitigation strategies and best practices in collaboration with NESCO
- Develop plans and facilitate testing security technologies in labs and pilot projects

- **Energy Sec. Selected for Creating and Running the Organization (NESCO)**
- **EPRI Led Team Selected for Providing Technical Resource (NESCOR)**

NESCO Program Structure

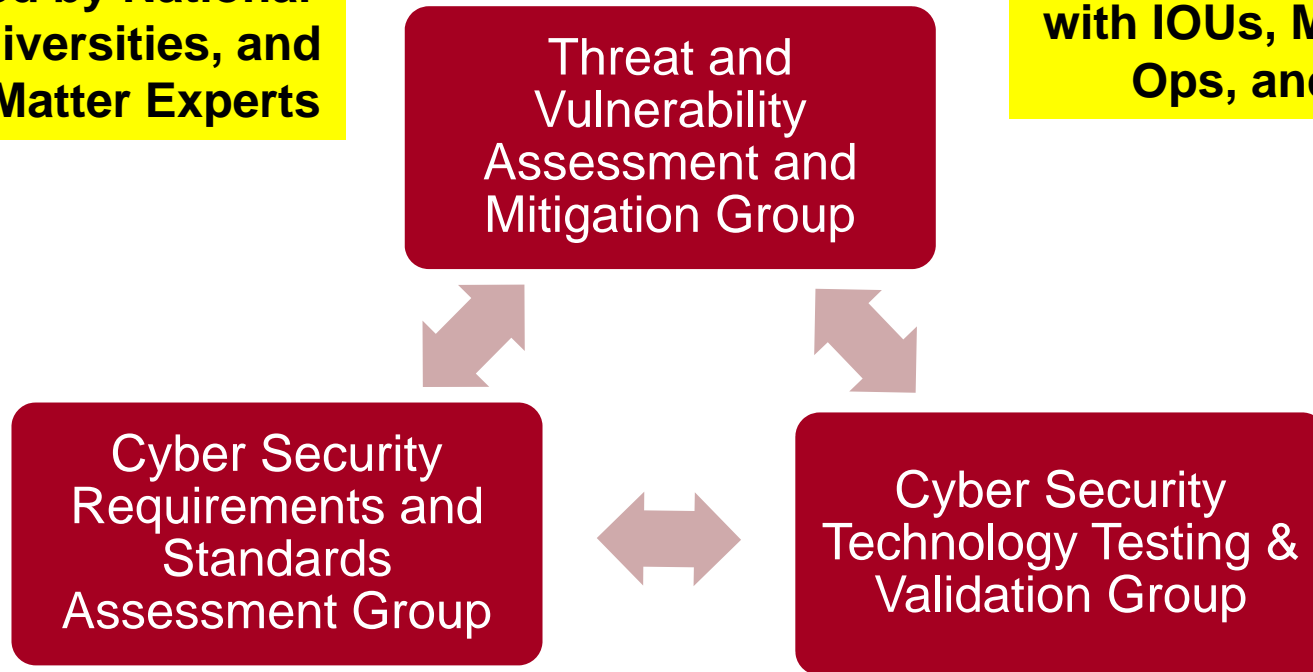
**EPRI has
created and
leads three
working groups**



NESCO Program Structure

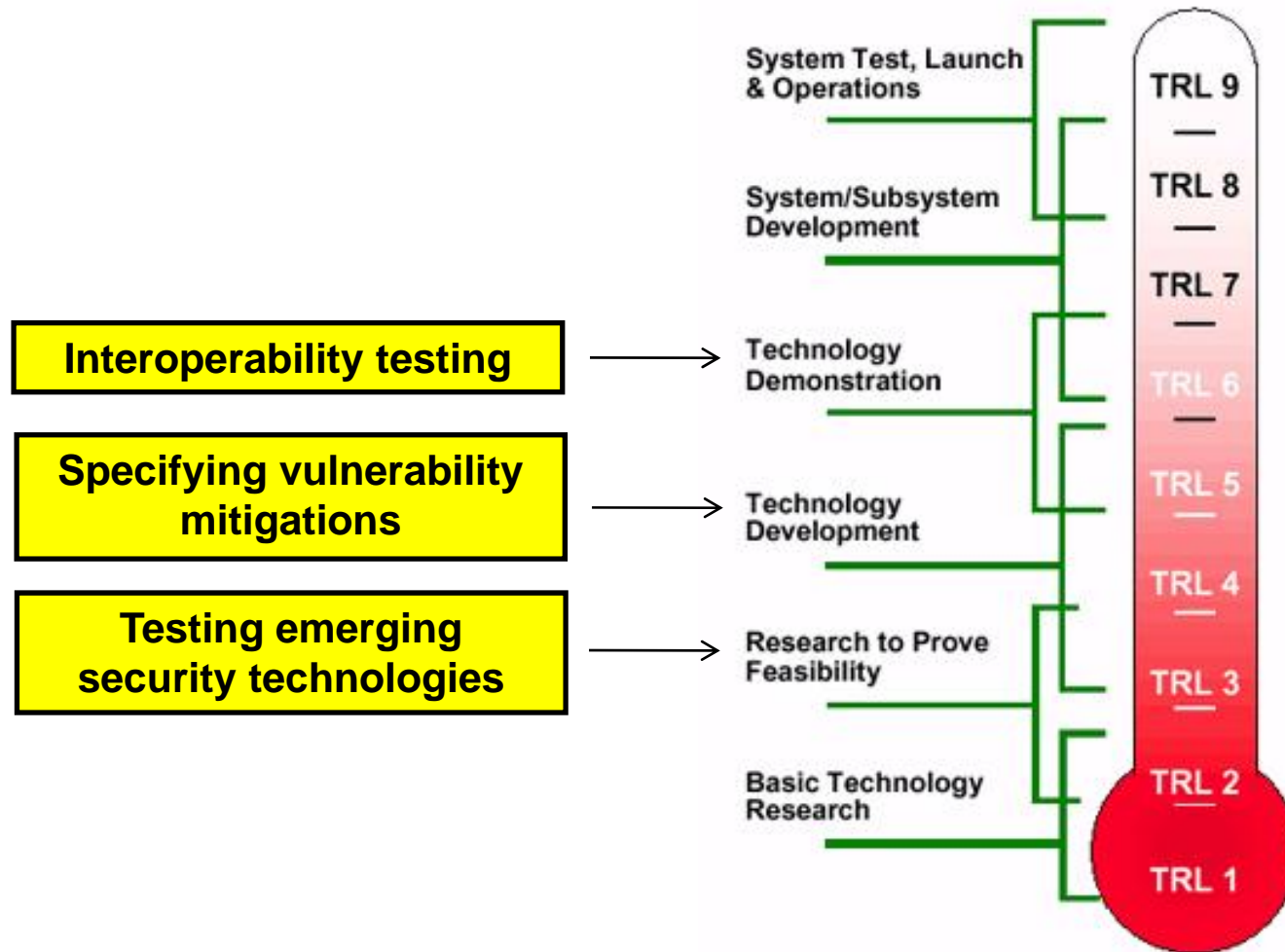
Working groups populated by National Labs, Universities, and Subject Matter Experts

Each WG collaborates with IOUs, Muni's, Co-Ops, and ISOs



Program to be advised by EPRI Cybersecurity Executive Committee

Technology Readiness Level



Transferring Research Into Sector

NESCOR seeds projects for the Cyber Security Program

Threat and Vulnerability Assessment and Mitigation Group

Developing risk mitigation strategies

Cyber Security Requirements and Standards Assessment Group

Cyber Security Technology Testing & Validation Group

Identifying security gaps

Transferring technology to industry

Group 1 R&D Activities for 2011

- Develop failure scenarios
 - Includes both malicious and non-malicious cyber security events
- Developed preliminary list of failure scenario topics at the NESCOR Annual Conference
 - Advanced metering infrastructure (AMI)
 - Distributed generation (DG)
 - Distributed energy resources (DER)
 - Demand response (DR)
 - Wide area monitoring, protection and control (WAMPAC)
 - Electric transportation (ET)
 - Other – including generation
- Developing criteria to prioritize failure scenario topics
- Develop prototype failure scenario

Group 2 R&D Activities for 2011

- Analyzing use cases with cybersecurity significance to identify interface requirements using NISTIR 7628 and “spaghetti diagram”
- Collecting non-functional requirements (end-to-end perspective)
- Mapping requirements to standards and procedures to identify gaps
 - Data Privacy
 - Remote Connect/Disconnect (AMI)
 - Customer Premises DER
 - Wide Area Monitoring Protection & Control (WAMPAC)

Group 3 R&D Activities for 2011

- Develop test plans for performing security assessments and penetration testing
 - Create a test plan template that can be adapted to specific Smart Grid applications
 - Develop test plan for AMI technician interfaces
 - Develop test plan for Wide-Area Measurement, Protection and Control systems



NESCOR Outreach Results in the Industry

- Cyber security subject matter experts from utilities, federal and state agencies, trade associations, integrators, vendors and individual contributors on the three technical working groups
 - Every other week conference calls for each task group
 - Volunteer time for technical work, provide industry perspective and share information
- Carried out a 2.5 day Annual Conference and workshop in Arlington VA June 29th – July 1st 2011 with 162 attendees representing various industry stakeholder groups to develop R&D project plans for all 3 NESCOR Groups
- Continuing to get the word out for increased collaboration

Contact Info

Erfan Ibrahim
EPRI Overall Project Lead &
Group 2 Lead
925 785-5967
eibrahim@epri.com

Annabelle Lee
Group 1 Lead
alee@epri.com

Galen Rasche
Group 3 Lead
grasche@epri.com

Frances Cleveland
Xanthus Consulting
Group 2 Co-lead
fcleve@xanthus-consulting.com

Justin Searle
UtiliSec
Group 3 Co-lead
justin@utilisec.com

Together...Shaping the Future of Electricity