EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Smart Grid Standards and Certification

June 27, 2012

Annabelle Lee

Technical Executive – Cyber Security

alee@epri.com

Current Environment

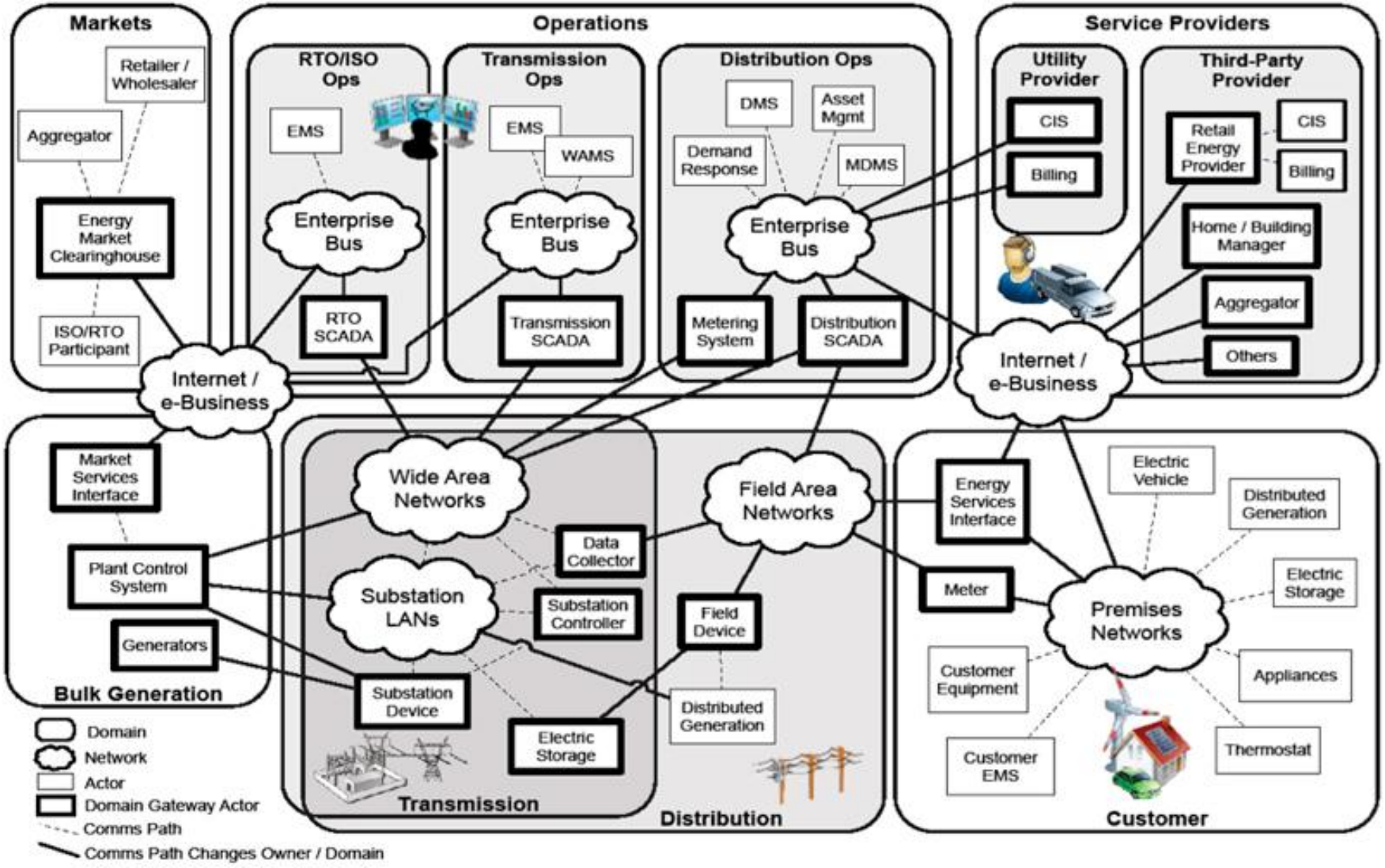
Current Grid Environment

- Legacy SCADA systems
- Limited cyber security controls currently in place
  - Specified for specific domains – bulk power distribution, metering
- Vulnerabilities might allow an attacker to…
  - Penetrate a network,
  - Gain access to control software, or
  - Alter load conditions to destabilize the grid in unpredictable ways
- Even unintentional errors could result in destabilization of the grid

Threats to the Grid

- Deliberate attacks
  - Disgruntled employees
  - Industrial espionage
  - Unfriendly states
  - Organized crime
  - Terrorists
- Inadvertent threats
  - Equipment failures
  - User/Administrator errors
- Natural phenomena
  - Weather – hurricanes, earthquakes
  - Solar activity

Interconnectedness of the Grid



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Trends Impacting Security

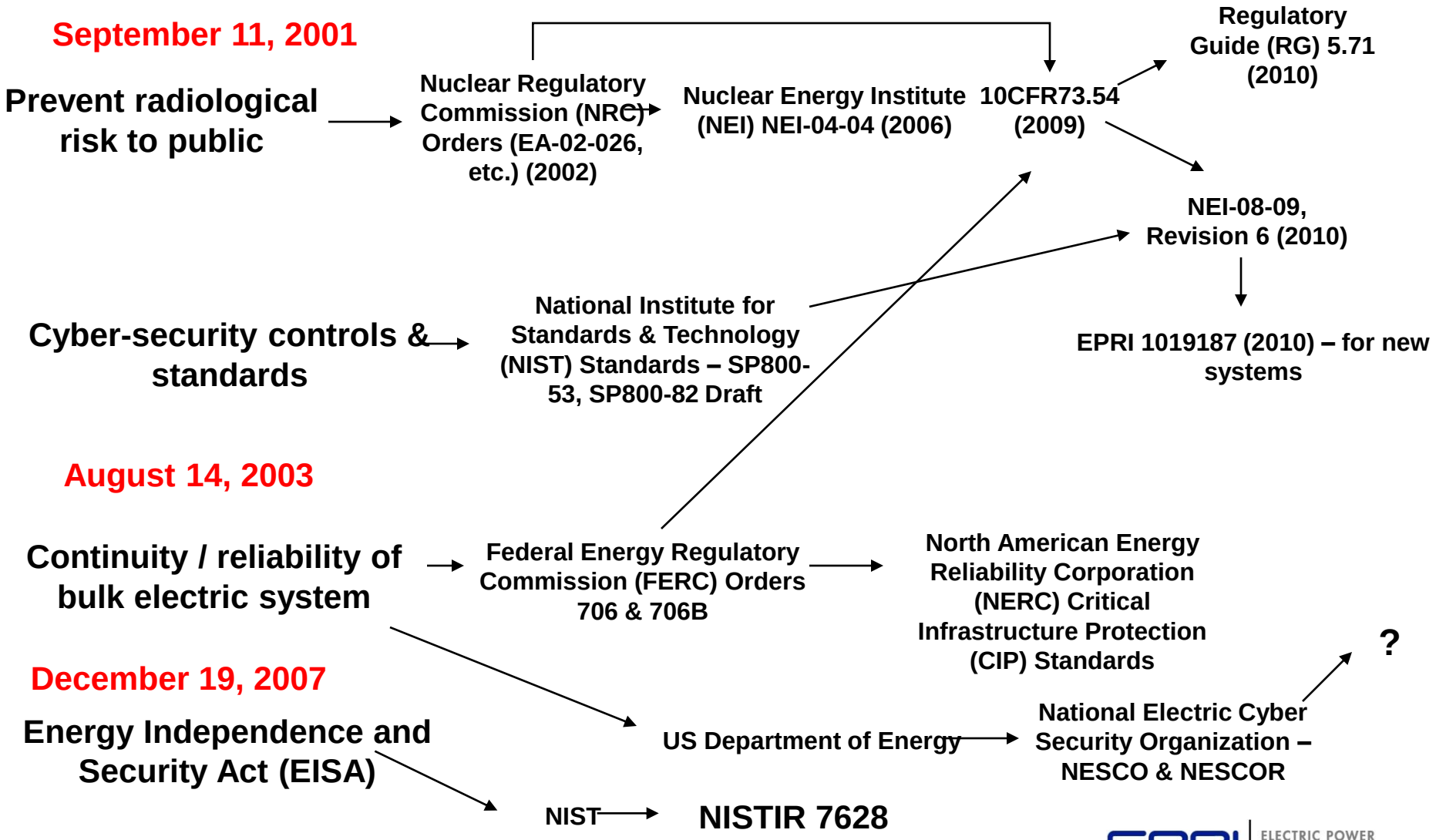
- Open protocols
  - Replacing vendor-specific proprietary communication protocols
- Connections with enterprise networks to obtain productivity improvements and information sharing
- Reliance on external communications
  - Increasing use of public telecommunication systems, the Internet, and wireless for control system communications
- Increased capability of field equipment
  - “Smart” sensors and controls with enhanced capability and functionality

IT and Control Systems – Differences…

- For IT systems, **confidentiality** and **integrity** are the major objectives
- For control systems, **availability** and **integrity** are the major objectives
- Limited bandwidth and processing capability
- Potential loss of life impact if there is a major compromise
- IT system life cycle varies from 6 months to 2 years
- Control systems life cycle varies from 15 to 40 years
- Availability
  - Delays usually accepted in IT systems
  - Control systems typically run 24/7/365

Regulatory Environment

Some Regulatory History…



Federal Energy Regulatory Commission (FERC) Technical Conference

- EISA directed FERC to:
  "institute a rulemaking to adopt such standards as may be necessary to ensure Smart Grid functionality and interoperability, after NIST's work has led to consensus in the Commission's judgment."

- NIST identified five families of standards as ready for consideration by regulators
  - Standards fundamental to Smart Grid interoperability
  - And to priorities identified in the Commission's July 16, 2009 Smart Grid Policy Statement

FERC Technical Conference (2)

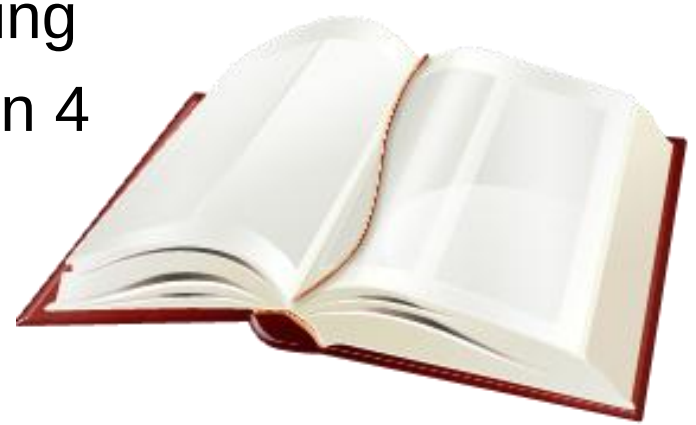
- Technical conference held January 31, 2011
- Unanimous agreement among speakers that the standards are not ready for adoption
- Additional questions posted on the website after the technical conference
  - http://www.ferc.gov/docs-filing/elibrary.asp
  - Under docket search, enter RM-11-2

FERC Decision

- On July 19, 2011 FERC issued an order related to the five families of standards:
  - "we [FERC] find insufficient consensus to institute a rulemaking proceeding at this time to adopt the five families of standards."
- At some future time, FERC could open a new docket and initiative rulemaking
  - This is based on the inclusion of the phrase "at this time…"
- FERC focused on stakeholder participation in the NIST interoperability framework process

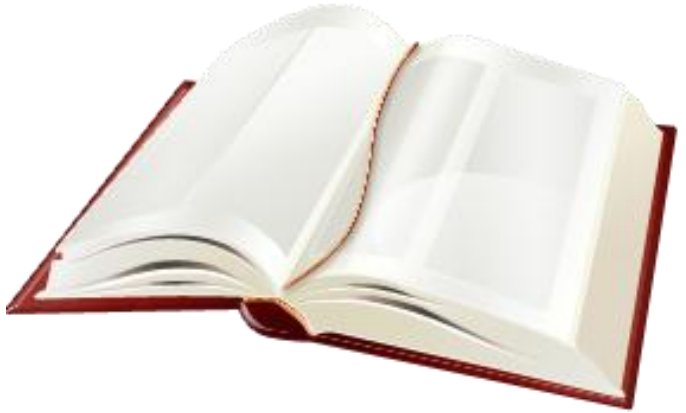
NERC Critical Infrastructure Protection (CIP) Version 4

- FERC Notice of Proposed Rulemaking
  - Docket No. RM11-11-000: Version 4 Critical Infrastructure Protection Reliability Standards
  - Posted September 15, 2011
  - FERC proposes to approve eight modified Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-4 through CIP-009-4
  - "Version 4" CIP Reliability Standards propose to modify CIP-002-4 to include "bright line" criteria for the identification of Critical Assets
    - 17 uniform bright line criteria



NERC Critical Infrastructure Protection (CIP) Version 4 (2)

- The proposed Version 4 CIP Reliability Standards would replace the currently effective Version 3 CIP Reliability Standards
- We (FERC) recognize that:
  - The Version 4 CIP Standards represent an “interim step” to addressing all of the outstanding directives set forth in Order No. 706



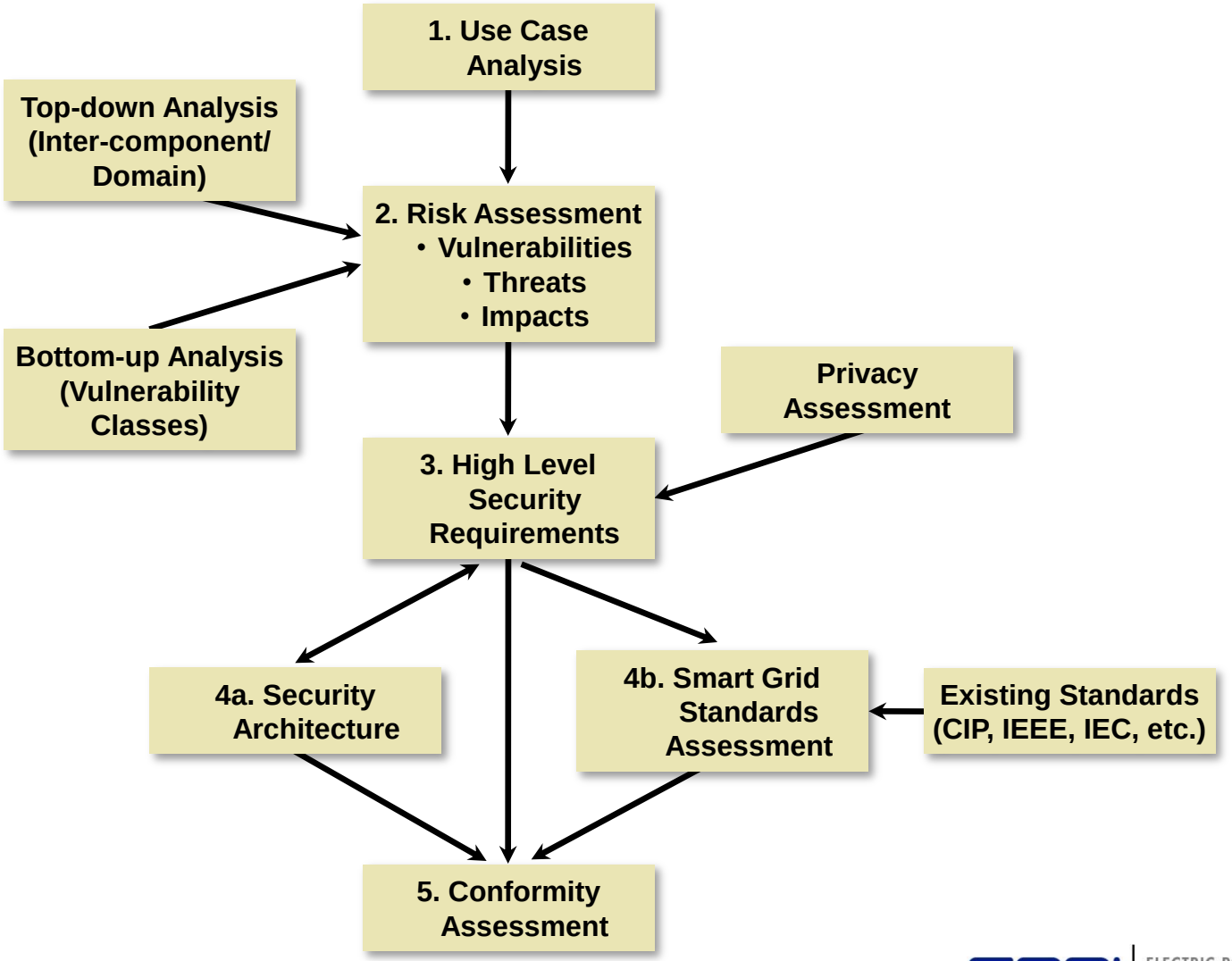
Cyber Security Strategies

NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*

- Version 1.0 published August 2010
  - http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628
- What it **IS**
  - A tool for organizations that are researching, designing, developing, and implementing Smart Grid technologies
  - May be used as a guideline to evaluate the overall cyber risks to a Smart Grid system during the design phase and during system implementation and maintenance
  - Guidance for organizations
    - Each organization must develop its own cyber security strategy (including a risk assessment methodology) for the Smart Grid
- What it **IS NOT**
  - It does not prescribe particular solutions
  - It is not mandatory

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 7628 – Smart Grid Cyber Security Strategy – Tasks



Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

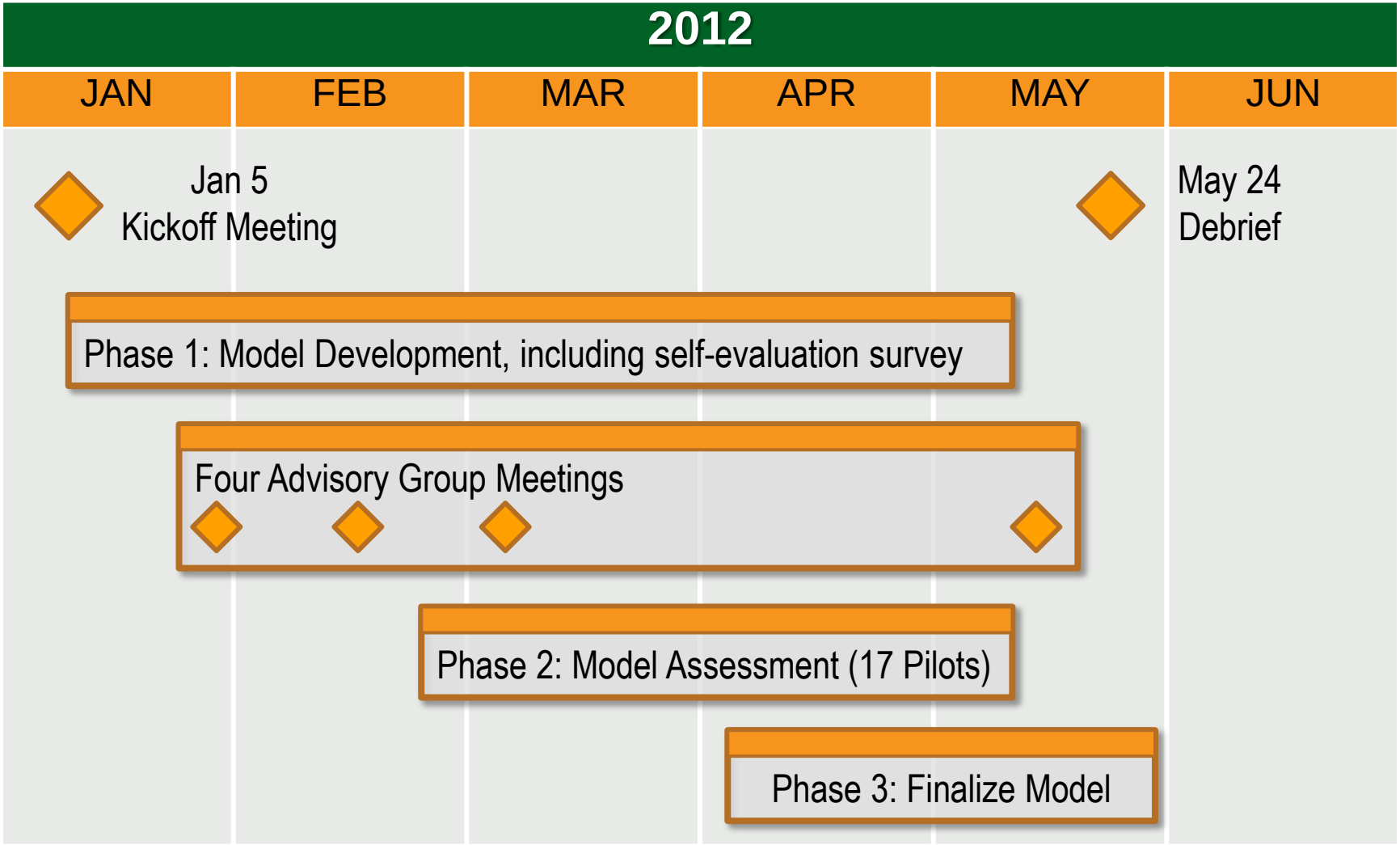
Initiative Background and Overview

- **Challenge**: Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid
- **Approach**: Develop a maturity model and self-evaluation survey to develop and measure cybersecurity capabilities
- **Results**: A scalable, sector-specific model created in partnership with industry

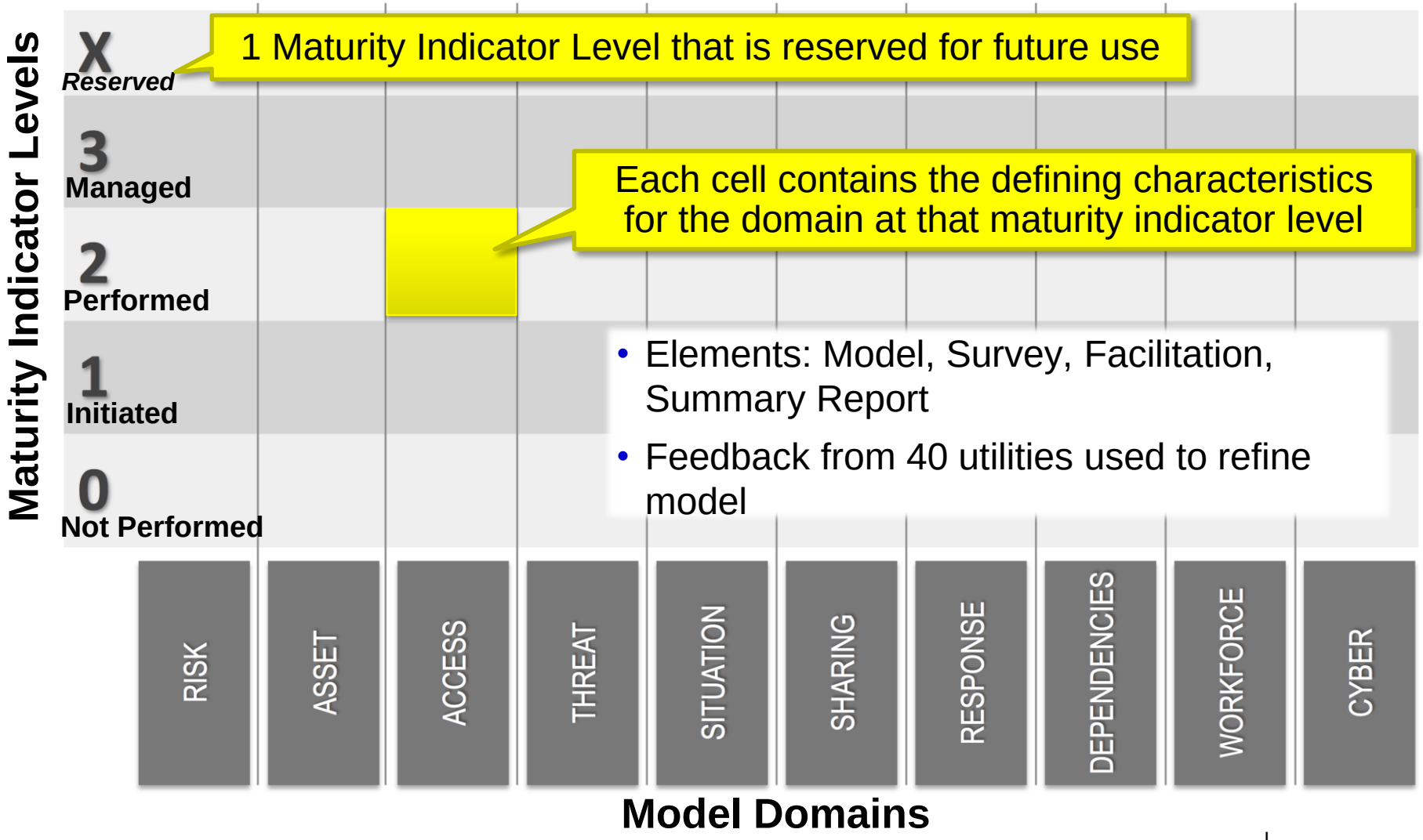
ES-C2M2 Objectives

- Strengthen cybersecurity capabilities
- Enable consistent evaluation and benchmarking of cybersecurity capabilities
- Share knowledge and best practices
- Enable prioritized actions and cybersecurity investments

ES-C2M2 Timeline



Model Overview



Moving Forward…

- Cyber security supports both the **reliability** and **privacy** of the Smart Grid
- Address **interconnected systems** – both IT and control systems
  - Cyber security needs to be addressed in all systems, not just critical assets
  - Augment existing reliability controls, as applicable
- Consider the **lifecycle** of IT/telecomm systems versus control systems
  - Patch management/update cycles
  - Product life cycle
  - Develop new models/paradigms for the two communities
- Continuously **assess** the security status

Moving Forward… (2)

- Acknowledge will be some security breaches
  - Focus on response and recovery
    - For example, isolate/quarantine infected devices
  - *Fail secure*
    - Address both safety and security
- Build security in!
  - Confidentiality, integrity and availability – implement best practices
- Apply IT/telecomm security lessons-learned from the past 40 years
- Train and educate
  - Address advanced persistent threats (APTs)
- Compliance DOES NOT equal security

Discussion

alee@epri.com

202.293.6345

Together…Shaping the Future of Electricity