U.S. Department of Energy

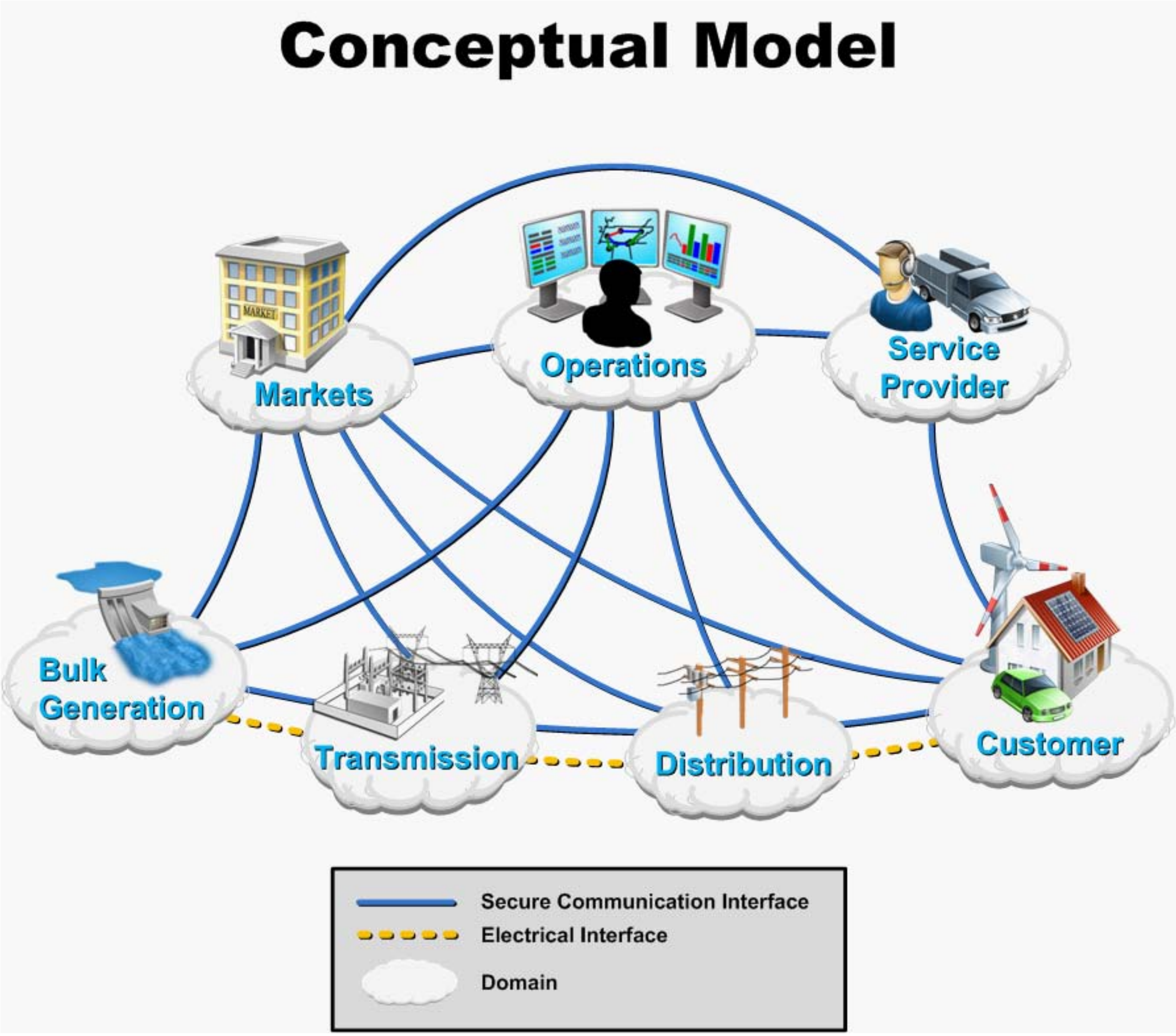
Office of Electricity Delivery and Energy Reliability

Smart Grid Investment Grant Program
(SGIG)

# *Cyber Security Issues and Requirements*

*Jeff Dagle*
*November 19, 2009*

# Communication and Information Technology will be Central to Smart Grid Deployment



Final Interim Smart Grid Roadmap, prepared by the Electric Power Research Institute (EPRI) for the National Institute of Standards and Technology (NIST)

# Cyber Security Requirements Associated with ARRA Projects

Proposals were required to include:

- Discussion of how cyber security risks will be mitigated
- What criteria will be used for vendor and technology selection
- Relevant cyber security standards that will be followed (or industry best practices)
- How emerging smart grid cyber security standards that are currently being developed will be adopted

# Cyber Security Objectives for Smart Grid Investment Grant Projects

- **Thorough, effective, and sustainable infrastructure protection posture**
- **Systems that are engineered with sufficient resiliency to absorb a failure, recover, and continue to provide critical functionality**
- **Deployable on a large scale, upgradeable on a continuous basis, and expandable without significant interruption in operations**

# Best Practices

- Good awareness of risk environment and how those risks would be mitigated
- Clearly identified cyber security responsibility
  - Good accountability and organizational support
  - Do not rely solely on 3rd party products/services
- Process selecting vendors based on security criteria
- Demonstrated which standards are appropriate
  - Rather than providing an exhaustive list of standards

# *Best Practices – Continued*

- Protection technology commensurate with infrastructure being protected
- Address design, deployment, maintenance, and operation of large-scale infrastructure protection systems that must run continuously for long periods of time
- Systematic approach to infrastructure protection
  - Leverage physical security to increase cyber security and vice versa
- Proactive Cyber Security
  - Conduct internal cyber security assessments on a routine basis
  - Established incident response team and procedures

# *Best Practices - Technical*

- Holistic approach – understand relationships and dependencies
- Secure network architectures, including defense in depth and compartmentalization
- Address confidentiality, integrity, availability requirements
  - Commensurate with the application
- Authorization and access control policies
- Auditing  & logging
- Configuration control & patch management
  - Does not require hands-on contact for remote devices or operational down-time

# *Bad Practices*

- Skipping the risk assessment and jumping straight in to providing long checklists of security measures
- Poor assumptions and sweeping generalities
  - Assumption that physical security provided cyber security
  - Assumption that upgrading equipment won’t increase risks
  - Broad dismissive statements (e.g., no new risks will be incurred, encryption can’t be broken)
- Overly reliant on 3rd party “shrink wrap” products and services
- Overly reliant on compliance to achieve infrastructure protection

# *Bad Practices - Continued*

- Mismatch between complexity and impact on system operations and the security of the control system
- Deployment of infrastructure protection technologies and tools without the necessary techniques in process and procedure that make them effective and sustainable
- A risk mitigation plan centered on one or two vulnerabilities or threats
- Cut and Paste: It was obvious when vendor marketing material was used out of context
  - Insufficient to provide checklist of technical specifications without an explanation of why the security mechanisms are put into place

# Path Forward

- Your assigned DOE Project Manager will work with your team to:
  - Provide specific feedback from your proposal evaluation including the cyber security review
  - Set expectations for cyber security implementation
- Key project milestones may be developed based on any specific cyber security concerns associated with your project
- DOE is developing on-line cyber security training
  - Anticipated to be available within 4-6 weeks
- Other resources to assist with the execution of the project are anticipated
  - For example, design reviews may be offered for high-risk projects
  - Specific details are still being worked out
- Your feedback and candid collaboration will be critical to achieving a successful outcome