Smart Grid

Overview and Cyber Security

October 23, 2009

Jim St Pierre

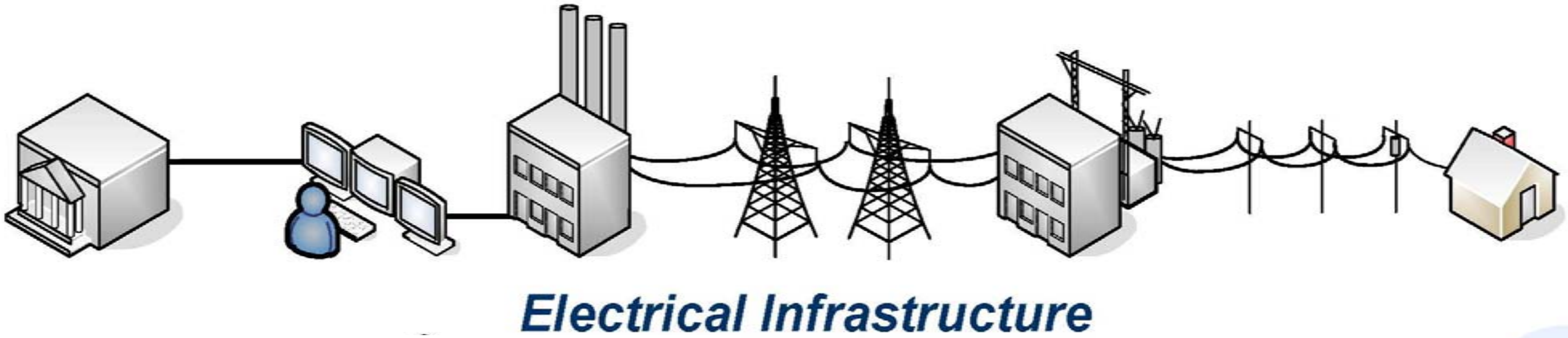
Deputy Director

Information Technology Laboratory

National Institute of Standards and Technology

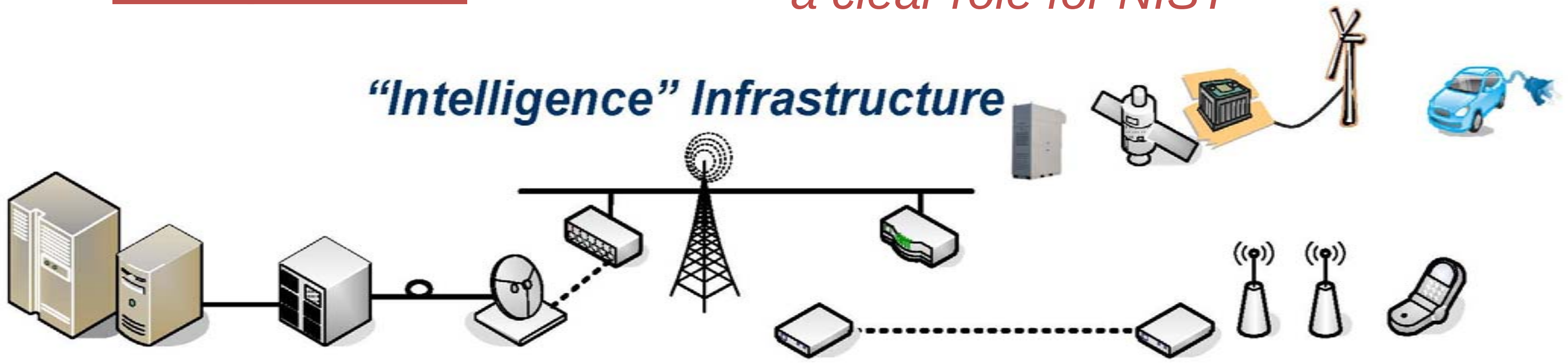
NIST
National Institute of
Standards and Technology

"Smart Grid" = Electric Grid + Intelligence



Combining electrical and information infrastructure requires interoperability…

Interoperability requires reliable standards and validated performance – *a clear role for NIST*



National Institute of Standards and Technology

Graphics courtesy of EPRI

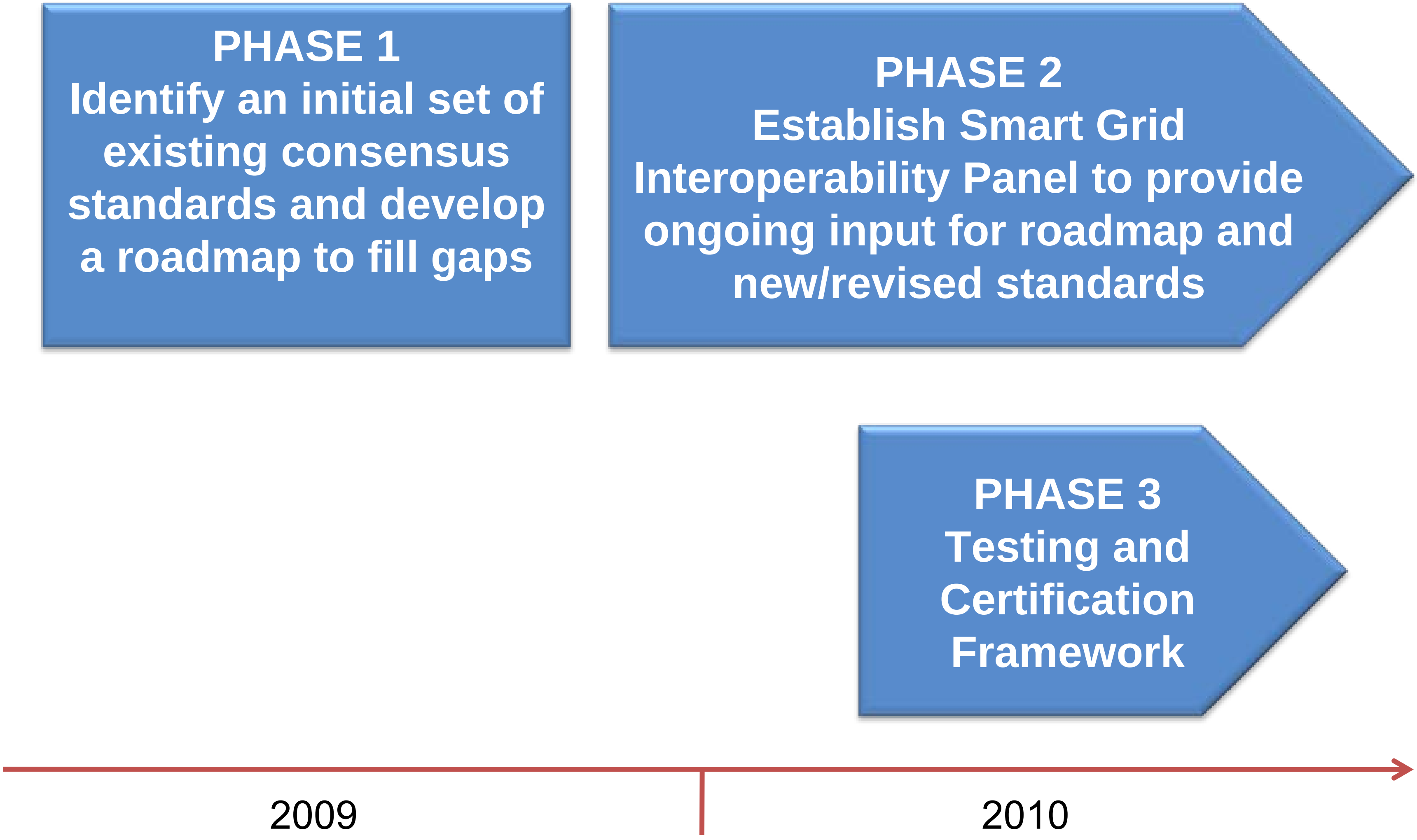
The NIST Role

Energy Independence and Security Act (EISA) of 2007
Title XIII, Section 1305.
Smart Grid Interoperability Framework

In cooperation with the DoE, NEMA, IEEE, GWAC, and other stakeholders, **NIST** has “primary responsibility to **coordinate development of a framework** that includes protocols and model standards for information management **to achieve interoperability of smart grid devices and systems**…”

NIST
National Institute of
Standards and Technology

NIST Three Phase Plan



PHASE 1
Identify an initial set of existing consensus standards and develop a roadmap to fill gaps

PHASE 2
Establish Smart Grid Interoperability Panel to provide ongoing input for roadmap and new/revised standards

PHASE 3
Testing and Certification Framework

2009

2010

March

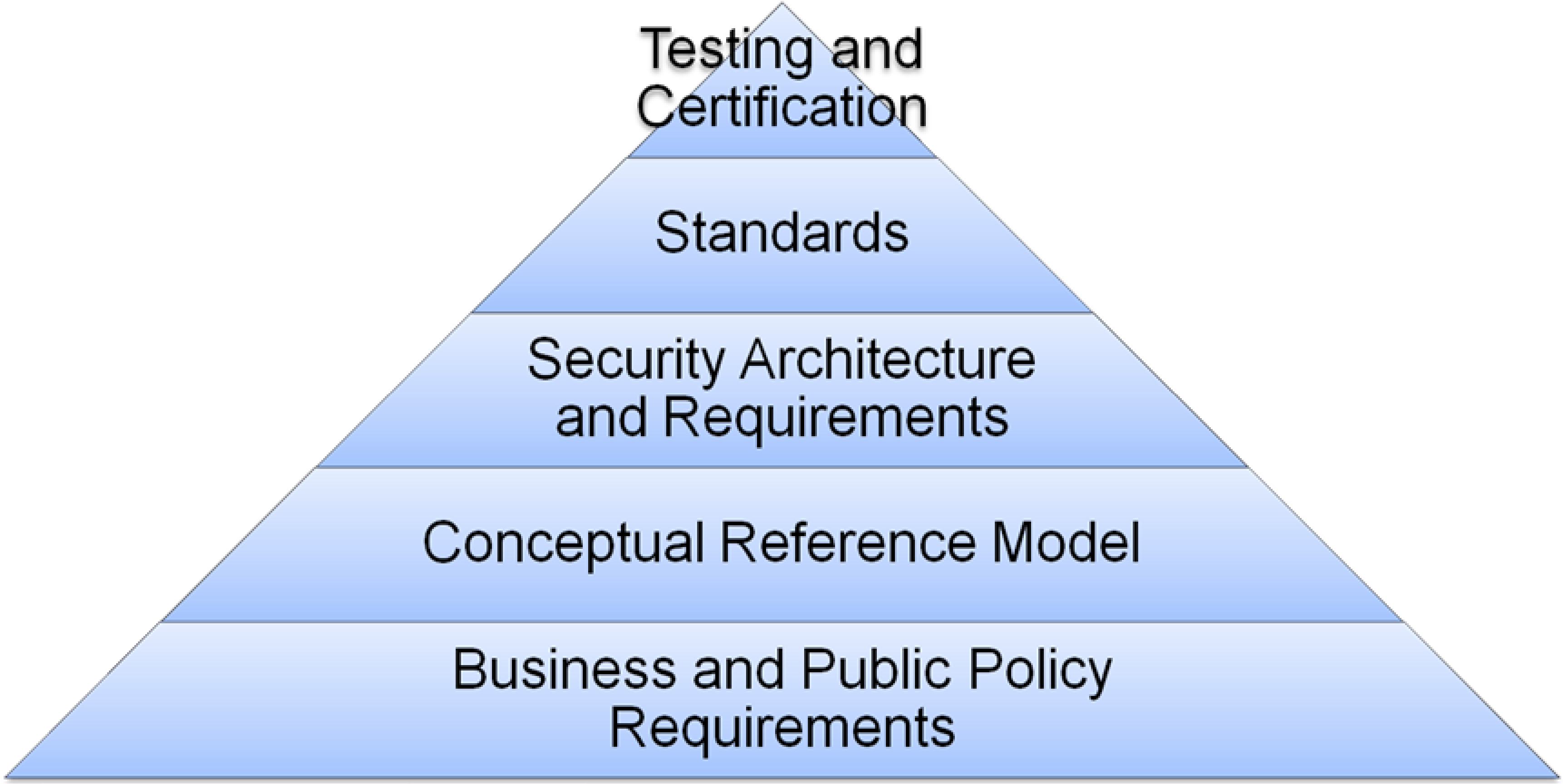
September

NIST
National Institute of Standards and Technology

Accelerated standards process

- Executives meeting with Secretaries Locke and Chu in May
- Workshops with more than 1500 participants
  - April 28-29, 2009
  - May 19-20, 2009
  - SDO Workshop, August 3-4, 2009
- EPRI Report, Priority Action Plans, Standards Organizations
- Comments through two Federal Register Notices
- On September 24, 2009, Secretary Locke announces availability of NIST Smart Grid Interoperability Framework and Roadmap, Release 1.0 (Draft) – GridWeek 2009
  - Request for public comment period open
  - Final version November 2009
- First meeting of Smart Grid Interoperability Panel - Nov 2009

Interoperability Framework Elements



Testing and Certification

Standards

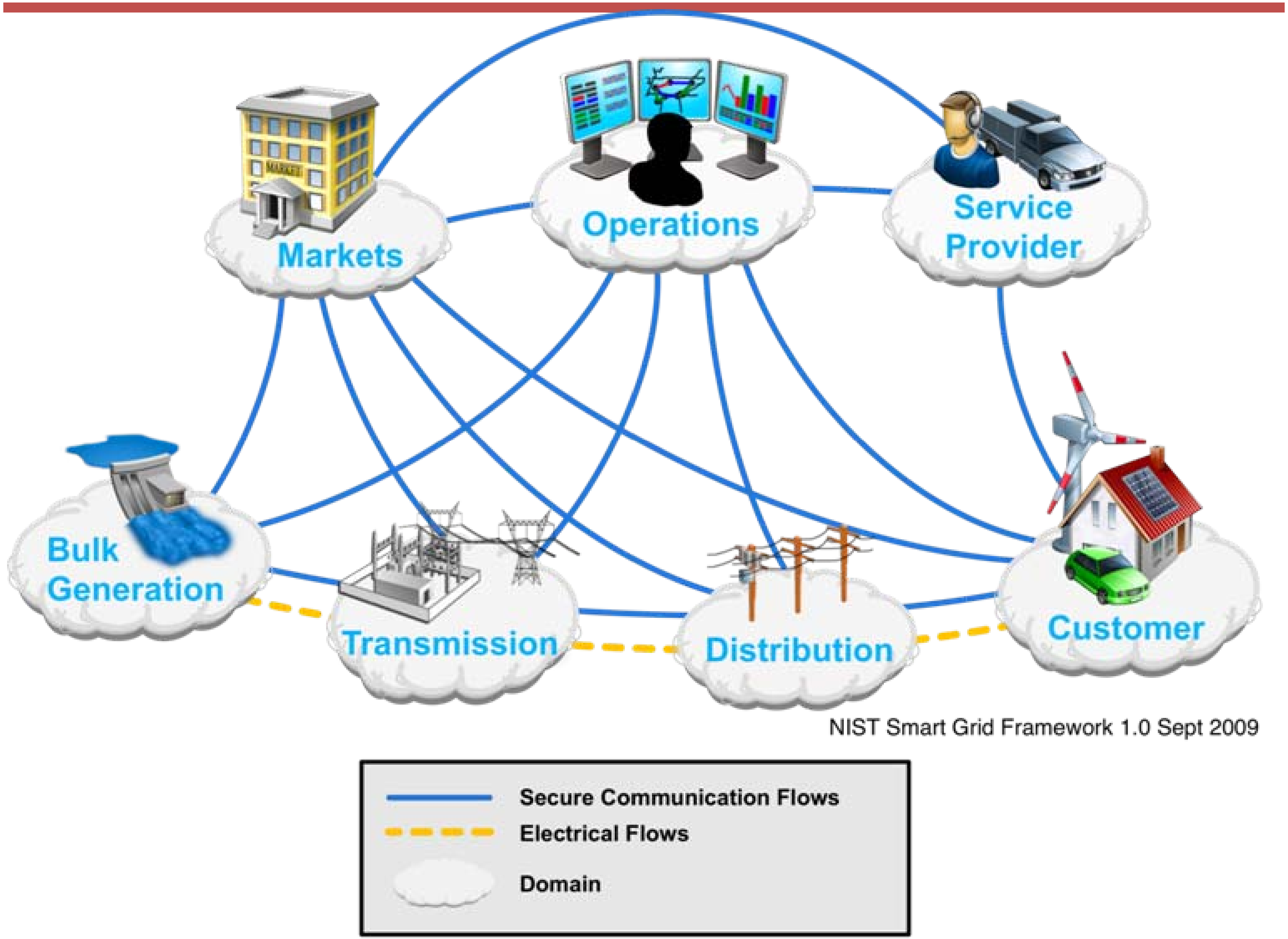
Security Architecture and Requirements

Conceptual Reference Model

Business and Public Policy Requirements

National Institute of Standards and Technology

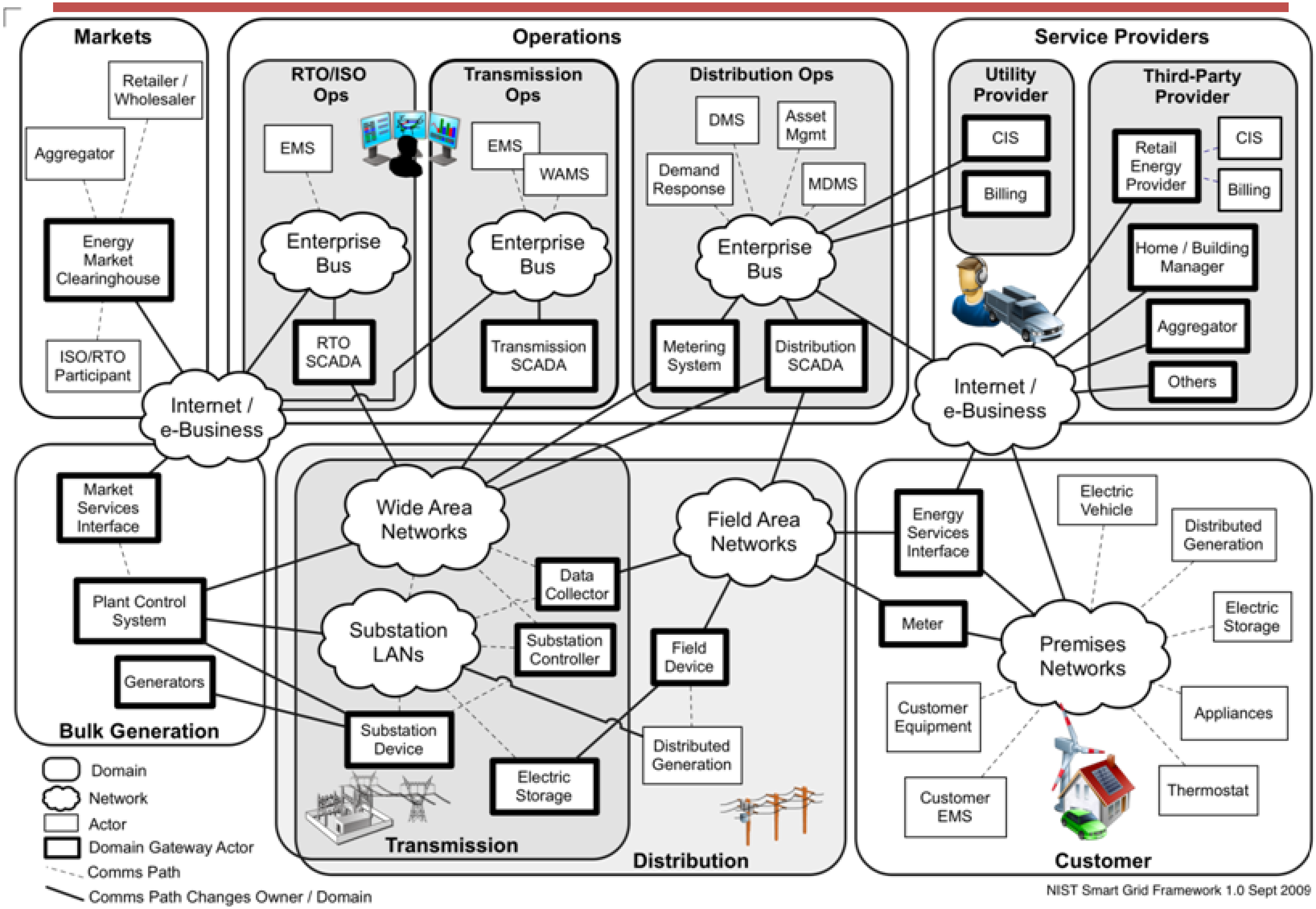
Smart Grid Domains



NIST Smart Grid Framework 1.0 Sept 2009

NIST
National Institute of Standards and Technology

Conceptual Reference Diagram



NIST Smart Grid Framework 1.0 Sept 2009

NIST
National Institute of Standards and Technology

Standards Identified

- Initial list of 16 has been expanded to 31
- 46 additional standards for further review
- Federal Register Notice published Oct 9

Guidance for Identifying Standards for Implementation

Some key considerations for evaluation of a standard for inclusion:

- Enables Smart Grid characteristic(s) as defined by EISA, DOE Smart Grid System Report
    - Is applicable to one of the priority areas identified by FERC and NIST
- Enables the transition of the legacy power grid to the Smart Grid.
- Is an open, stable and mature industry-level standard developed in consensus processes from a standards development organization (SDO)
- Is supported by an SDO or Users Group to ensure that it is regularly revised and improved to meet changing requirements and that there is strategy for continued relevance.

Guidance for Identifying Standards for Implementation (2)

- Is openly available under fair, reasonable, and nondiscriminatory terms.
- Is developed and adopted internationally, wherever practical

Priorities for Standardization

- Demand Response and Consumer Energy Efficiency
- Wide Area Situational Awareness
- Electric Storage
- Electric Transportation
- Advanced Metering Infrastructure
- Distribution Grid Management
- Cyber Security
- Network Communications

What are Priority Action Plans (PAPs)

- NIST workshops identified priority standards issues
  - many standards require revision or enhancement
  - and new standards need to be developed to fill gaps
- A total of 70 priority standards issues were identified in the EPRI report
- NIST determined which require most urgent resolution and selected top 14 to initiate PAPs
- The August SDO Workshop was used to develop the action plan for each priority issue.
- Current status for each PAP is posted on the NIST website
  - broad SDO and stakeholder support and participation
  - aggressive milestones in 2009 or early 2010 established

What are Priority Action Plans (PAPs) (2)

- NIST and the Smart Grid Interoperability Panel will guide and oversee progress on PAPs and development of new PAPs.

Priority Action Plans	Target Date
Smart meter upgradeability standard	completed
Common specification for price and product definition	early 2010
Common scheduling mechanism for energy transactions	year-end 2009
Common information model for distribution grid management	year-end 2010
Standard demand response signals	January 2010
Standard for energy use information	January 2010
IEC 61850 Objects / DNP3 Mapping	2010

NIST
National Institute of
Standards and Technology

Priority Action Plans (continued)	Target Date
Time synchronization	mid-2010
Transmission and distribution power systems models mapping	year-end 2010
Guidelines for use of IP protocol suite in the Smart Grid	mid-year 2010
Guidelines for use of wireless communications in the Smart Grid	mid-year 2010
Electric storage interconnection guidelines	mid-2010
Interoperability standards to support plug-in electric vehicles	December 2010
Standard meter data profiles	year-end 2010

Information Networks

- Network of networks to improve the control and management of energy generation, distribution and consumption, and the current state of grid interconnectivity so that information can flow between the various actors in the Smart Grid.
- Thorough analyses and guidelines - to be developed in the context of the priority actions plans - will determine the suitability of IP-based networks and choice of communication technologies used for various Smart Grid applications and requirements.
- Access points from the public Internet to the utility networks pose potential risks that need to be analyzed and mitigated.

IP PAP : Role of IP in the Smart Grid

Major tasks include:

- Developing a set of networking requirements for different Smart Grid applications
- Identifying a Core Protocol Suite for IP-based Smart Grid
- Identifying additional protocols or protocol enhancements beyond the core suite required by a specific class of applications
- Develop guidelines for IP-based Smart Grid deployment
- Identifying new protocol or protocol enhancement standardization activities required to fully support Smart Grid in the future

Wireless PAP : develop guidelines for the use of wireless communications in the Smart Grid

Major tasks include:

- Segmenting the Smart Grid application domains into wireless environments/groups with similar sets of requirements
- Creating an attribute list and performance metrics for wireless standards
- Creating an inventory of wireless technologies and standards that are identified by each SDO
- Conducting an evaluation of the wireless technologies based on the application requirements
- Performing a gap analysis and developing guidelines for the use of wireless technologies.

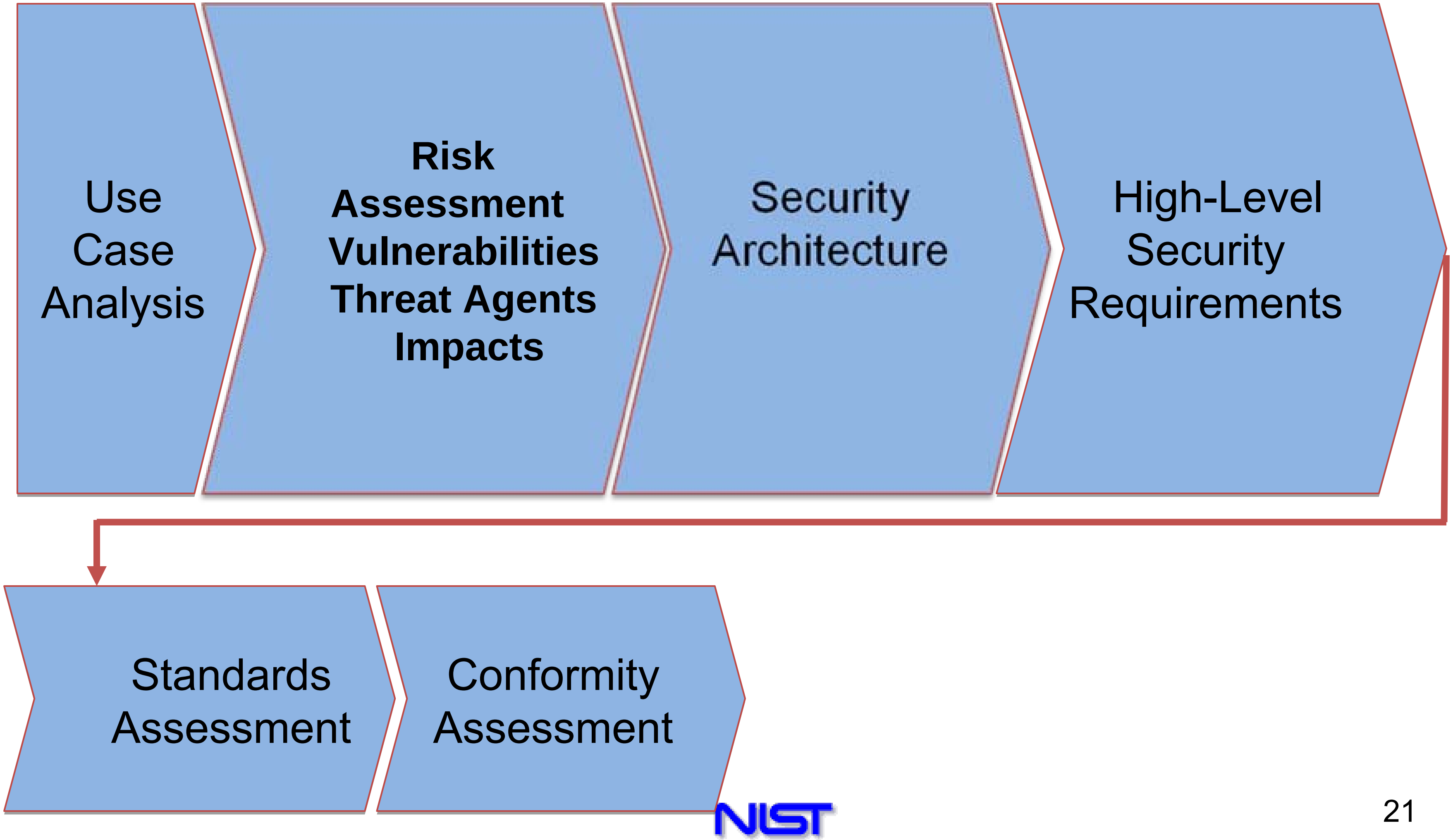
NIST
National Institute of
Standards and Technology

Completed Priority Action Plan

- NEMA Smart Grid Standard AMI 1-2009, Requirements for Smart Meter Upgradeability

- Start of work to approved standard: 90 days!

Cyber Security Work Program


Use Case Analysis
Risk Assessment Vulnerabilities Threat Agents Impacts
Security Architecture
High-Level Security Requirements
Standards Assessment
Conformity Assessment

Current Grid Environment

- Legacy SCADA systems
- Security by obscurity
- 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

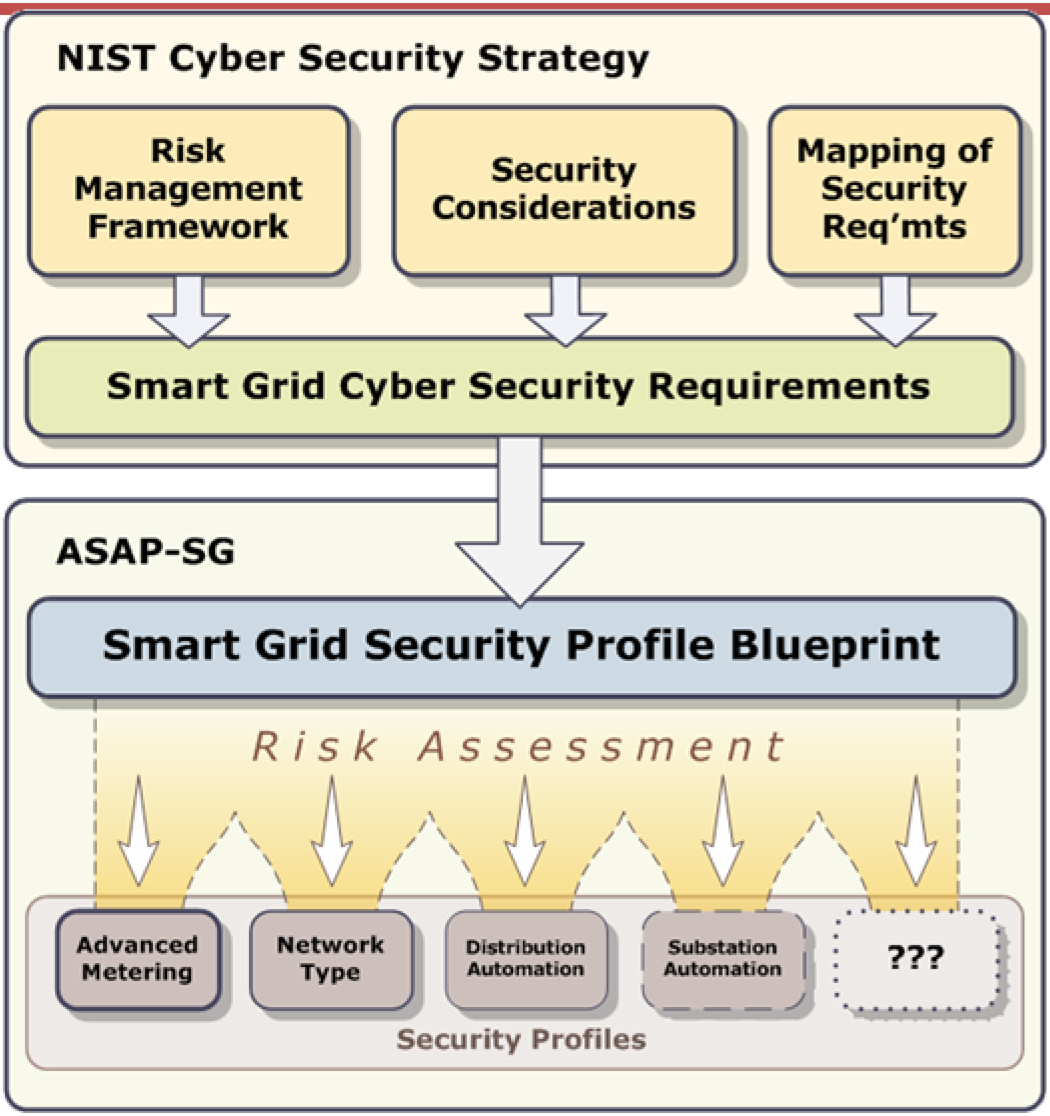
Smart Grid Cyber Security Strategy

- Establishment of a Cyber Security Coordination Task Group (CSCTG)
  - Over 250 participants
    - Private sector – vendors, service providers
    - Academia
    - Regulatory organizations
    - Federal agencies
  - Have established several sub-working groups
    - Vulnerability class analysis
    - Bottom-Up assessment
    - Privacy
    - Standards assessment
    - High level requirements
    - Functional architecture development

Smart Grid Cyber Security Strategy (2)

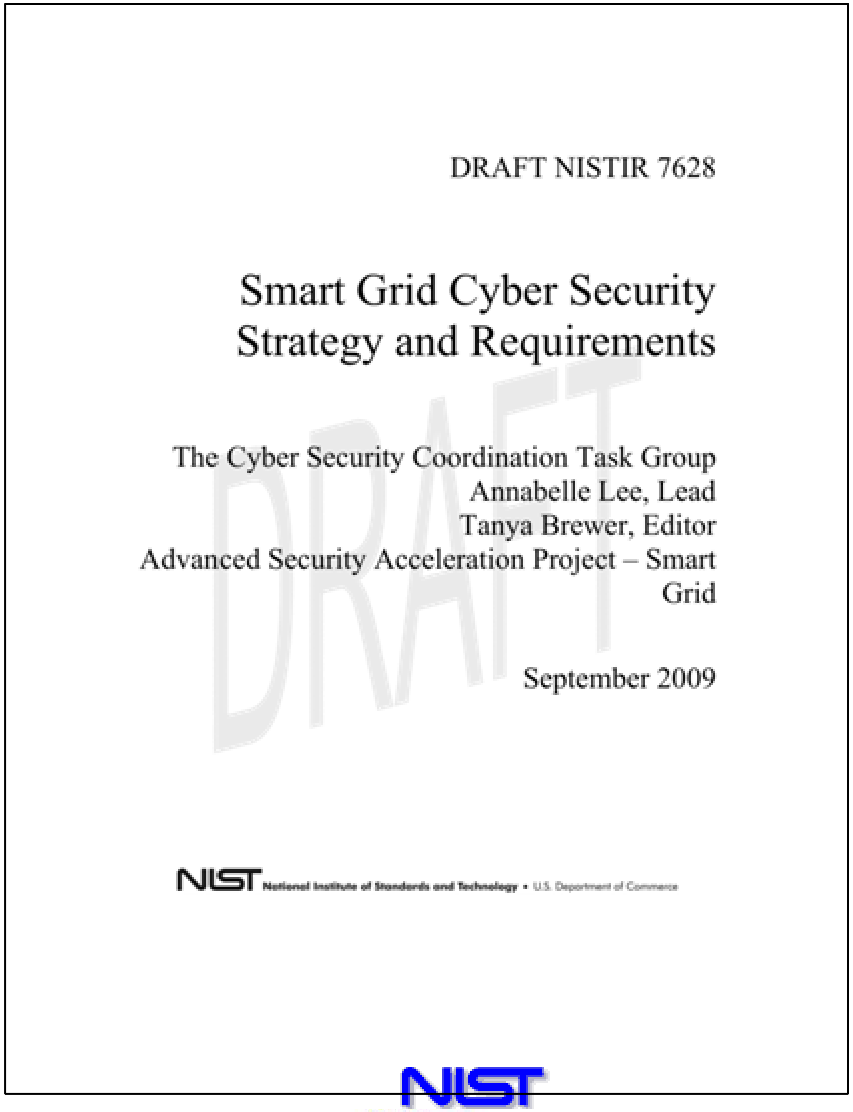
  - Weekly telecon
- The strategy…
  - Selection of use cases with cyber security considerations
  - Performance of a risk assessment of the Smart Grid, including assessing vulnerabilities and impacts
  - Development of a security architecture linked to the Smart Grid interface diagrams
  - Identification of cyber security requirements and risk mitigation measures to provide adequate protection
- The final product
  - A set of recommended cyber security requirements

NIST Cyber Security Strategy Coordination with the Advanced Security Acceleration Project – Smart Grid


NIST Cyber Security Strategy
Risk Management Framework
Security Considerations
Mapping of Security Req'mts
Smart Grid Cyber Security Requirements
ASAP-SG
Smart Grid Security Profile Blueprint
Risk Assessment
Advanced Metering
Network Type
Distribution Automation
Substation Automation
???
Security Profiles

National Institute of Standards and Technology

Smart Grid Cyber Security Strategy and Requirements



DRAFT NISTIR 7628

Smart Grid Cyber Security
Strategy and Requirements

The Cyber Security Coordination Task Group
Annabelle Lee, Lead
Tanya Brewer, Editor
Advanced Security Acceleration Project – Smart Grid

September 2009

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

NIST
NIST
National Institute of Standards and Technology

Smart Grid Cyber Security Strategy and Requirements Draft

- First draft posted as a NIST Interagency Report (NISTIR) 7628
  - Development of the document lead by NIST
  - Document written by the CSCTG and the Advanced Security Acceleration Project – Smart Grid team
  - Represents significant coordination among federal agencies, the private sector, regulators, and academics
  - Document includes material that will be used in selecting and tailoring the security requirements
    - Included material may also be used by system implementers
- First draft has been posted for a 60-day comment period
  - http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf

NIST
National Institute of Standards and Technology

Smart Grid Cyber Security Strategy and Requirements Draft (2)

  - Comments due by December 1, 2009
- Current plan is to publish a second draft at the end of December 2009
  - Second draft will also be posted for a 60-day comment period
  - Draft will include
    - Revisions based on submitted comments
    - High level requirements for the entire Smart Grid
    - Overall functional architecture and draft security architecture
    - Initial assessment of standards
- Final version planned for publication in March 2010
  - Will address all comments

NIST
National Institute of Standards and Technology

NISTIR 7628

- The draft NISTIR includes the following sections:
  - Overall cyber security strategy for the Smart Grid
    - Risk assessment process
    - Tasks and deliverables
  - Privacy and the Smart Grid
    - Initial assessment of the privacy issues
  - Logical interface analysis – initial analysis
    - Six functional priority areas diagrams with logical interfaces defined
    - Allocation of logical interfaces to categories
    - Identification of security constraints and issues for each category
    - Specification of confidentiality, integrity, and availability impact levels (low, moderate, high) for each category

NISTIR 7628 (2)

- The draft NISTIR includes the following sections (2):
  - Advanced Metering Infrastructure (AMI) security requirements
    - Developed by the ASAP-SG team – many members also part of the CSCTG
  - Crosswalk of cyber security documents
    - Cyber security standards and requirements documents for IT and control systems
  - Key power system use cases with security considerations
    - Extracted from several sources and security considerations added
  - Vulnerability categories
    - Aggregation of specific vulnerabilities identified from several sources

NISTIR 7628 (3)

- The draft NISTIR includes the following sections (2):
  - Bottom-Up analysis of cyber security issues
    - Detailed analysis of specific issues and gaps identified
- Members of the CSCTG and the ASAP-SG
- Acronyms List

How to Participate

- NIST Smart Grid portal: http://nist.gov/smartgrid
- Cyber Security Coordination Task Group
  - Lead: Annabelle Lee (annabelle.lee@nist.gov)
- Cyber Security Twiki site:
- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

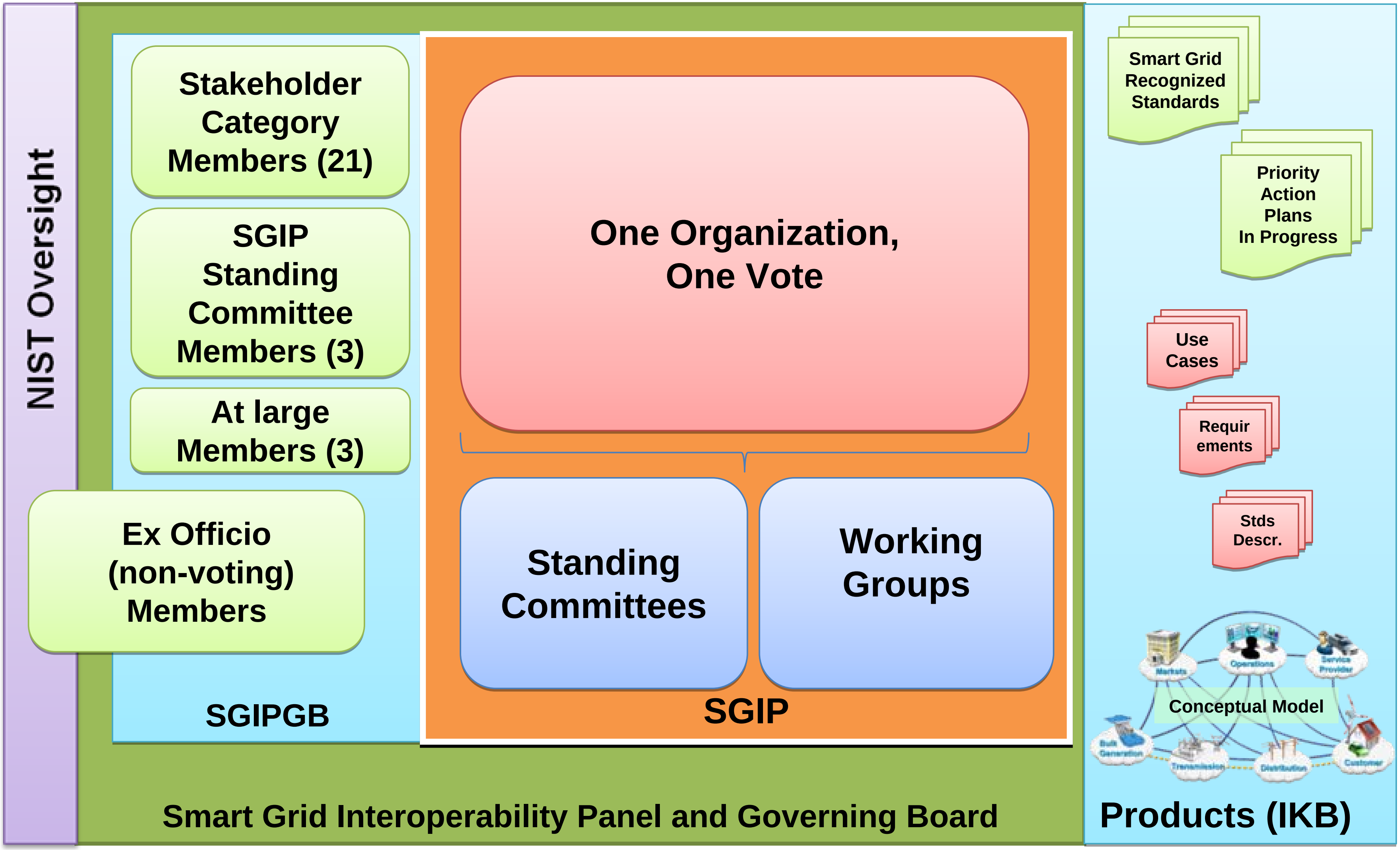
SG Interoperability Panel (SGIP): Vision

- Public-private partnership to support NIST EISA responsibility
- Open, transparent body
- Representation from all SG stakeholder groups
- Membership open to any materially interested stakeholder
- Not dominated by any one group
- SGIP does not directly develop or write standards
  - Stakeholders participate in the ongoing coordination, acceleration and harmonization of standards development.
  - Reviews use cases, identifies requirements, coordinates conformance testing, and proposes action plans for achieving these goals.

SG Interoperability Panel (SGIP): Vision (2)

- SGIP has a Governing Board
  - Approves and prioritizes the work of the Panel
  - Coordinates necessary resources (in dialog with SDOs, user groups, and others) to carry out finalized action plans in efficient and effective manner.
- SGIP has key foundational committees and ad hoc working groups
  - SG Architecture Committee
  - SG Testing and Certification
  - Activities of Domain Expert Working Groups transitioned into SGIP Working Groups as appropriate

SGIP Structure



NIST Oversight

Stakeholder Category Members (21)

SGIP Standing Committee Members (3)

At large Members (3)

Ex Officio (non-voting) Members

SGIPGB

One Organization, One Vote

Standing Committees

Working Groups

SGIP

Smart Grid Interoperability Panel and Governing Board

Smart Grid Recognized Standards

Priority Action Plans In Progress

Use Cases

Requirements

Stds Descr.

Conceptual Model

Products (IKB)

SGIP: Stakeholder Categories

1.	Investor Owned Utilities
2.	Municipal Electric Utilities
3.	Rural Electric Associations
4.	Independent Power Producers
5.	Renewable Power Producers
6.	Independent System Operators/ Regional Transmission Organizations
7.	Retail Service Providers
8.	Commercial & Industrial Consumers
9.	Residential Consumers
10.	IT, Application Developers & Integrators
11.	ICT Infrastructure Providers
12.	Electric Transportation

SGIP: Stakeholder Categories (2)

13.	Equipment Manufacturers and Vendors
14.	Testing and Certification Vendors
15.	Electricity & Financial Market Traders
16.	Venture Capital
17.	Standard Development Organizations
18.	Professional Societies, User Groups, Industry Consortia
19.	Academia, R&D Organizations
20.	State & Local Regulators
21.	Relevant Federal Agencies

National Institute of Standards and Technology

SGIP: Testing and Certification

Smart Grid Testing and Certification is the third phase of the NIST Smart Grid 3-Phase Plan

- Key Principles:
  - Leverage existing work where possible
  - Provide a structure to coordinate existing testing programs and fill gaps
  - Ensure proper coordination with SDOs

SGIP: Timeline

- Late August: NIST awarded Phase 2 contract to EnerNex to support the establishment and administration of SGIP
- Soliciting input from SG community on ongoing basis
  - Now – late October is key opportunity for input
  - Webinar series (first one Oct 9, additional ones Oct 28, Nov 12)
- First SGIP meeting planned during week of November 16
  - Co-located with Grid-Interop '09 in Denver, Colorado
- Post SGIP Charter
- Publish NIST requirements for Governing Board members
- Candidate Evaluation Team prepares Governing Board member ballot

SGIP: Timeline (2)

- Post Governing Board Ballot and Final Draft Charter November 11
- Governing Board candidates on ballot presented at Grid-Interop, November 17
- SGIP organization members electronically cast ballots November 17-18 COB
- SGIP Charter ratified by November 19

Feedback Mechanisms

- NIST would like your input
- All materials on NIST SG TWiki
  - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome
- NIST email address: smartgrid@nist.gov, “SGIP:” to start subject line