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

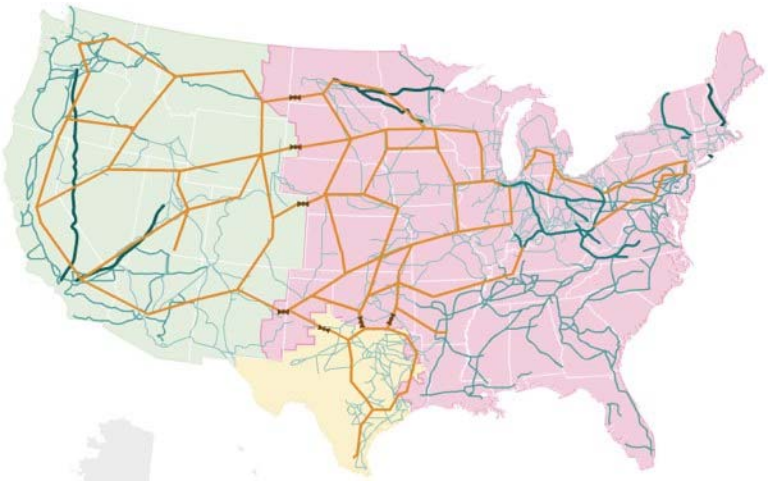
NIST and the Smart Grid

Annabelle Lee
Senior Cyber Security Strategist
National Institute of Standards and Technology
U.S. Department of Commerce
11 January 2010

Why Do We Need Smart Grids?

Fundamental Drivers

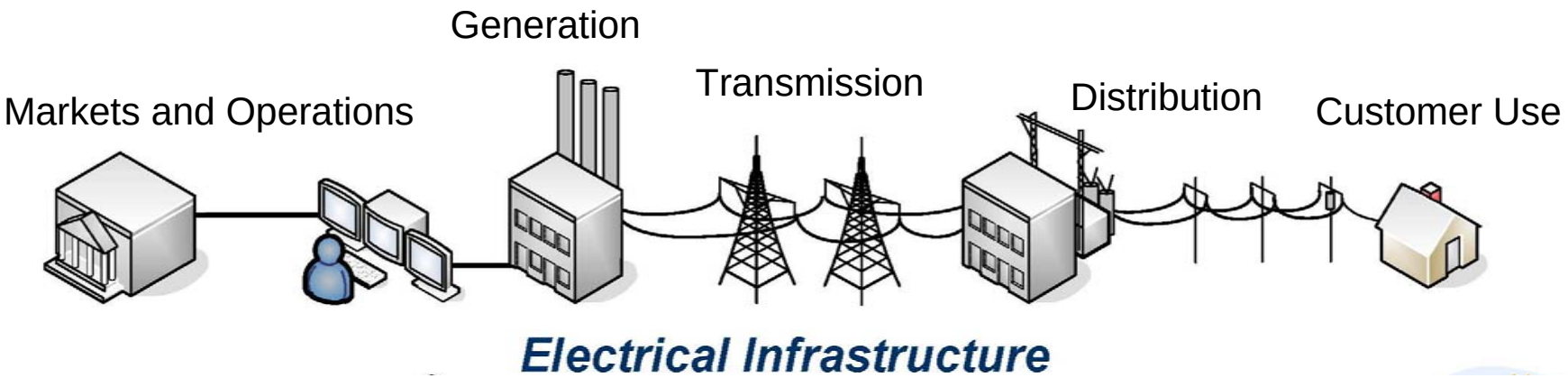
- Climate change
- Energy security
- Lifestyle dependent on electricity
- Jobs



Smart Grid goals

- Reduce energy use overall and increase grid efficiency
- Increase use of renewables (wind and solar don't produce carbon)
- Support shift from oil to electric transportation
- Enhance reliability and security of the electric system

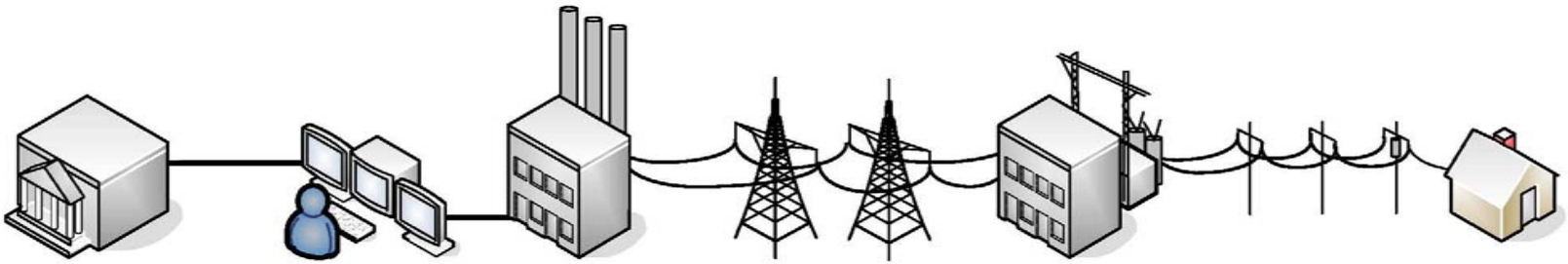
Today's Electric Grid



One-way flow of electricity

Centralized, bulk generation
Heavy reliance on coal and oil
Limited automation
Limited situational awareness
Consumers lack data to manage energy usage

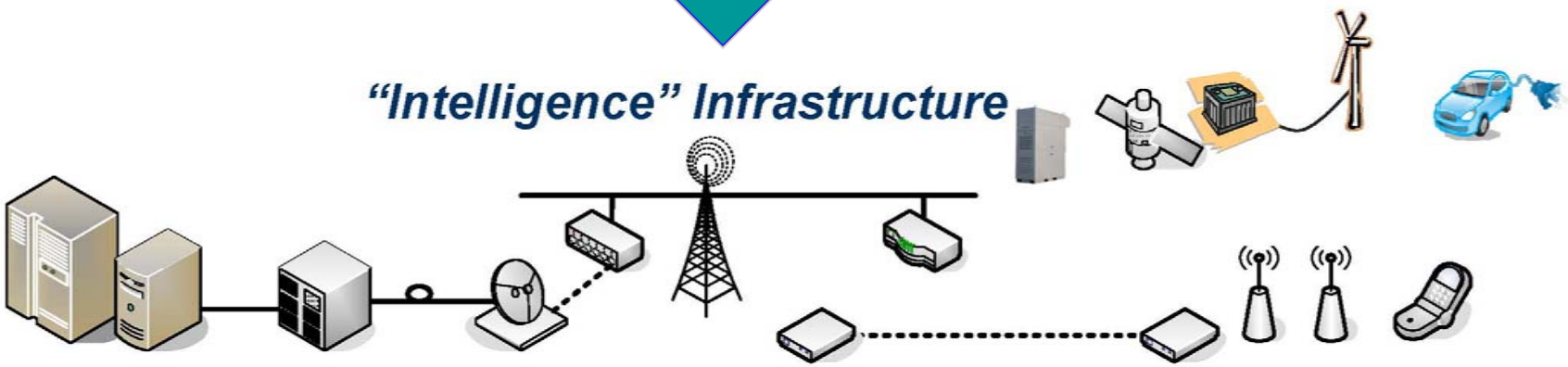
Smart Grid: The "Enernet"



Electrical Infrastructure

2-way flow of electricity and information

"Intelligence" Infrastructure



Graphics courtesy of EPRI

NIST National Institute of Standards and Technology

Energy Independence and Security Act

Defines ten national policies for the Smart Grid:

1. Use digital technology to improve reliability, security, and efficiency of the electric grid
2. Dynamic optimization of grid operations and resources, with full cyber-security
3. Integration of distributed renewable resources
4. Demand response and demand-side energy-efficiency resources
5. Automate metering, grid operations and status, and distribution grid management
6. Integrate “smart” appliances and consumer devices
7. Integrate electricity storage and peak-shaving technologies, including plug-in electric vehicles
8. Provide consumers timely information and control
9. Interoperability standards for the grid and connected appliances and equipment
10. Lower barriers to adoption of smart grid technologies, practices, and services.

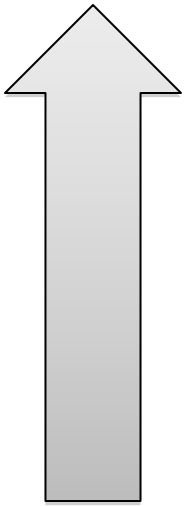
The NIST Role

- Coordinate the interoperability framework by identifying the protocols and model standards necessary to enable the Smart Grid vision as outlined in the 2007 Energy Independence and Security Act (EISA) Title XIII mandate

  - Work with industry stakeholders to achieve a common vision and consensus on the necessary standards
  - Report on progress in the development of the interoperability framework
  - Work with standards bodies/users groups to get standards harmonized/developed & used
  - **Visible active federal government leadership and coordination by NIST**

Government Roles in Smart Grid

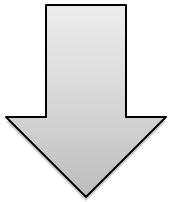
Federal



U.S. DEPARTMENT OF ENERGY

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

Federal Energy Regulatory Commission



State

Public Utility Commissions

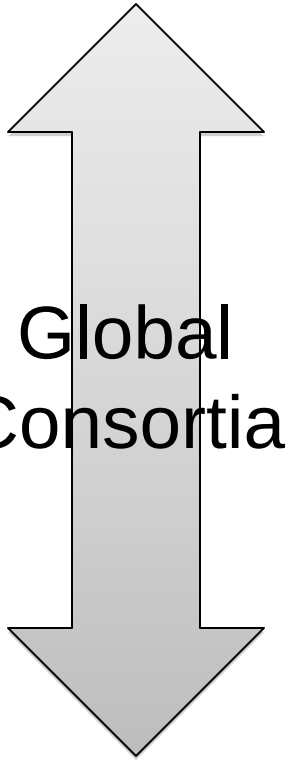
Why Do We Need Standards?

Whirlpool Corporation To Produce One Million Smart Grid-Compatible Clothes Dryers by the End of 2011…

Standards for data communication, price information, schedules, demand response signals

Standards Come From Many Sources

International



Global Consortia

Regional and National

IEC

ISO

ITU

IETF

IEEE

SAE International

ZigBee Alliance

OGC
Open Geospatial Consortium, Inc.

OASIS

ANSI
American National Standards Institute

SAE

NAESB

NEMA

NIST
National Institute of Standards and Technology

The Need for Standards is Urgent

Example: Smart Meters

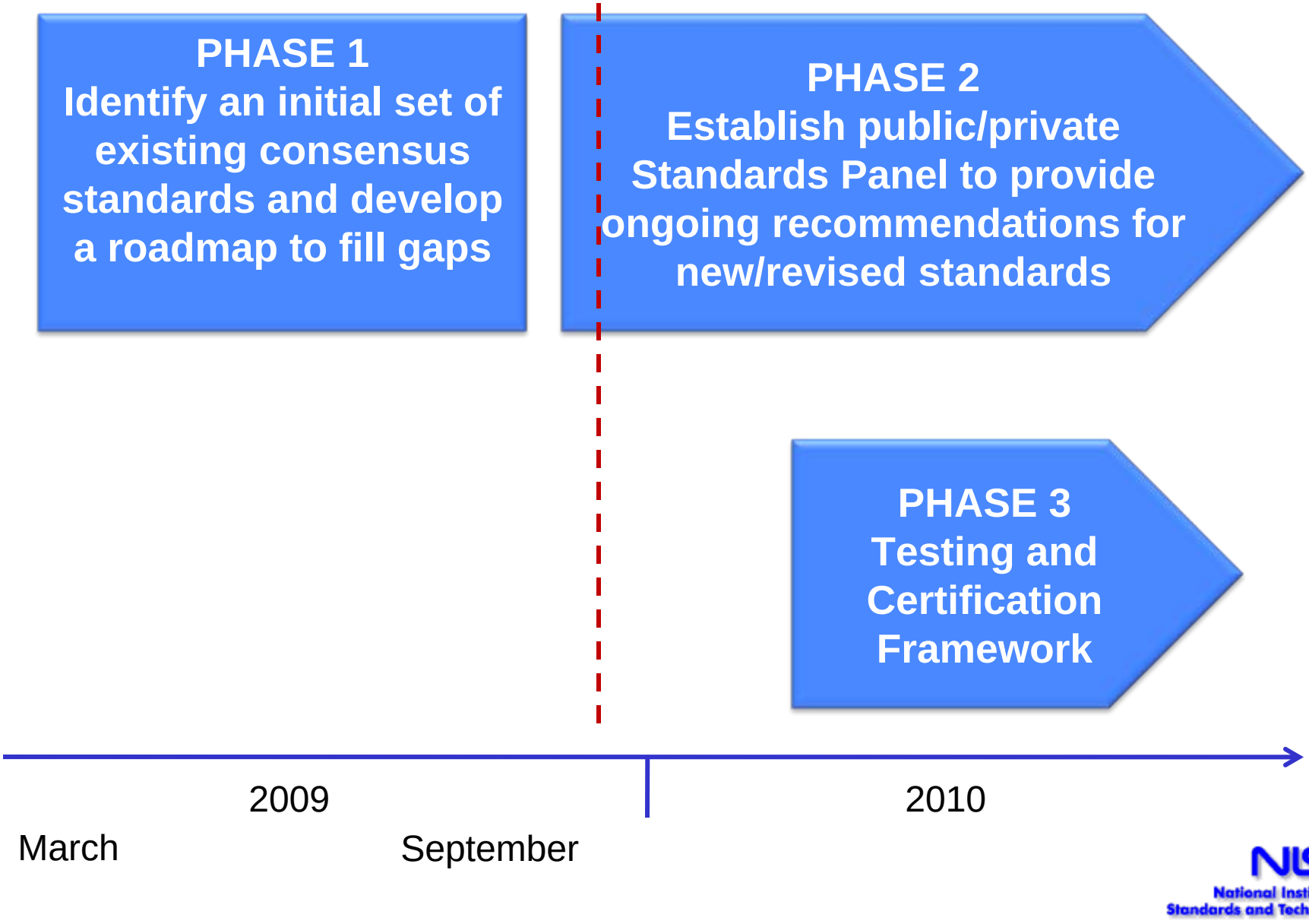
- Key element of smart grids
- 40 million to be deployed in the next several years in US
- Rapid technology evolution
- Absence of firm standards

White House Meeting May 18, 2009

- Chaired by Secretaries of Energy and Commerce
- 66 CEOs and senior executives, federal and state regulators

- Commitment to accelerate development of a roadmap

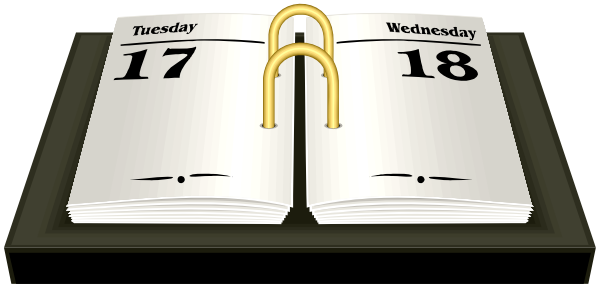
NIST Three Phase Plan



NIST
National Institute of Standards and Technology

NIST Smart Grid Timeline

- 2007 ***EISA gives NIST responsibility*** for a Smart Grid Framework
- 2008 NIST forms ***Domain Expert Working Groups***
  - T&D, Home-to-Grid, Building-to-Grid, Industry-to-Grid, Business and Policy, Cyber
- 2009 ***ARRA accelerates*** need for standards
  - EPRI selected as contractor
- 2009 NIST holds ***large-scale workshops*** to identify standards
  - Over 1500 participants from a variety of groups
  - April 28-29: Produced draft list of 16 standards: "low hanging fruit"
  - May 19-20: Analyzed use cases, requirements and standards
  - August 3-4: Developed Priority Action Plans with SDO representatives
- 2009 August ***EPRI assembles Roadmap Report*** from workshops
- 2009 September
  - ***NIST Smart Grid Framework draft 1.0*** released
  - ***NIST Smart Grid Cyber Security Strategy and Requirements draft*** released
  - EnerNex selected as contractor for next phases
- 2009 November
  - ***Smart Grid Interoperability Panel*** *established*
- 2009 December
  - First meeting ***Governing Board*** Dec 8-9, 2009 at NIST
- 2010 January
  - ***NIST Smart Grid Framework 1.0***



NIST
National Institute of Standards and Technology

NIST Smart Grid Timeline

- Dec 2007 – Energy Independence and Security Act
- Aug 2008 – NIST forms Domain Expert Working Groups w/GWAC
- Nov 2008 – NIST Workshop at Grid-Interop 2008 in Atlanta

2009

January

February

March

April

May

June

July

August

September

October

November

December

- Feb 17 – American Reinvestment and Recovery Act
- Mar 19 – FERC Smart Grid Policy Statement and Action Plan
- George Arnold: National Coordinator for SG Interoperability

NIST Smart Grid Interoperability Roadmap
Workshops and Development

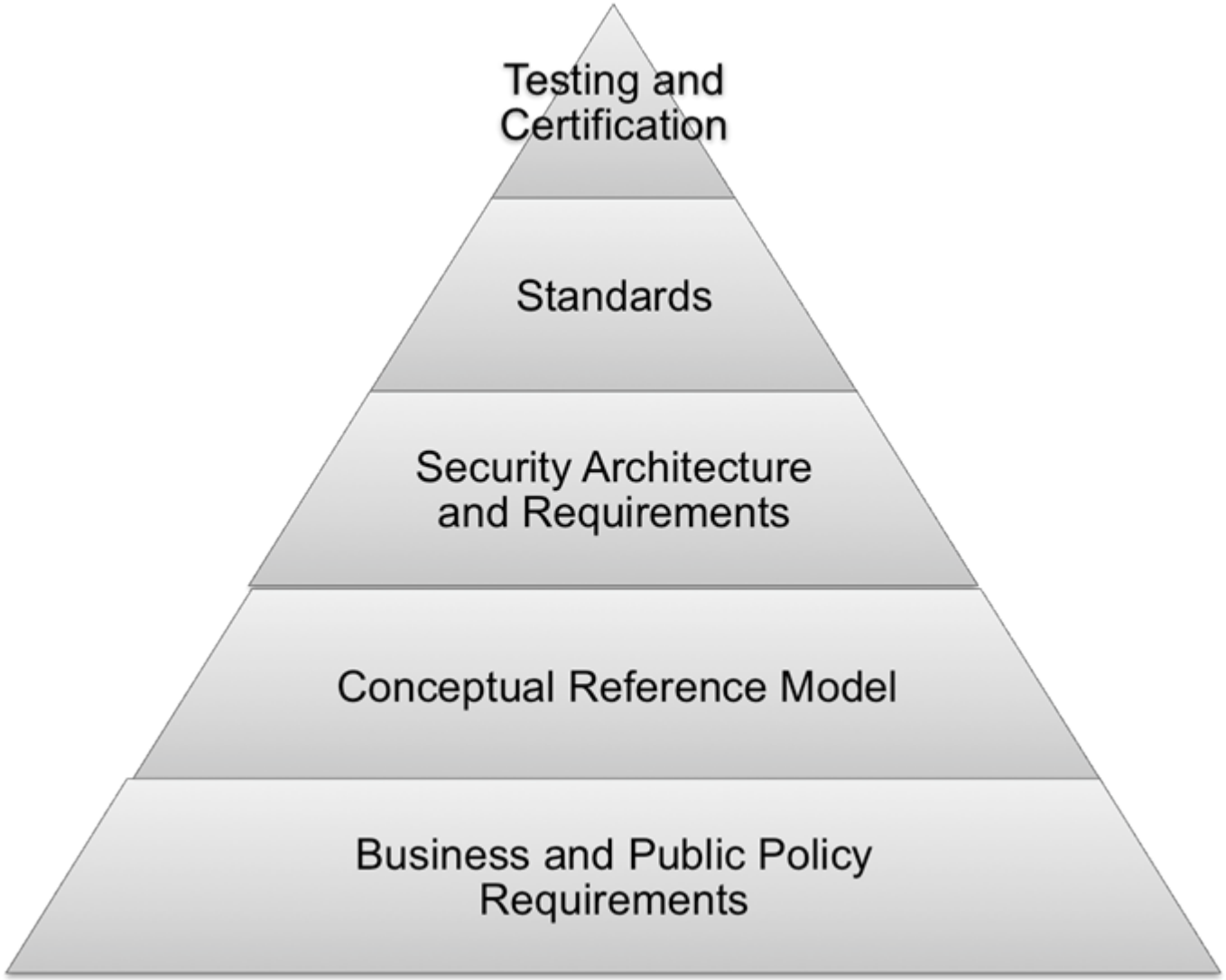
Priority Action Plans & SGIP Charter Development (to Nov 12)

- NIST Smart Grid Interoperability Framework 1.0 Draft
- SGIP Update Webinars – Oct 9, Oct 28, Nov 12
- SGIP Inaugural Meeting November 16-19
  - Charter Ratified
  - Governing Board First Meeting Dec 8-9

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

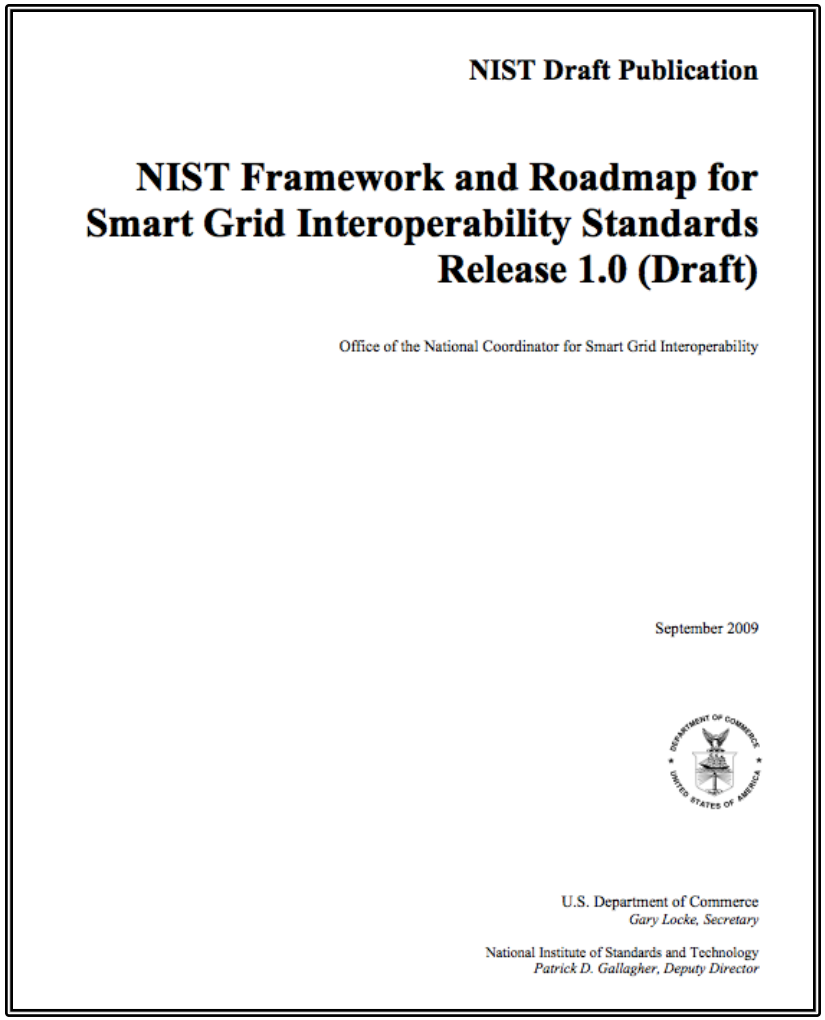
Interoperability Framework



NIST National Institute of Standards and Technology

Draft Release 1.0 Framework

- Smart Grid Vision
- Reference Model
- Over 70 standards identified
- Priority action plans to fill gaps
- Cyber security strategy
- Next steps



NIST Draft Publication

NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)

Office of the National Coordinator for Smart Grid Interoperability

September 2009

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

NIST
National Institute of Standards and Technology

SGIP Vision

- Public-private partnership to support NIST EISA responsibility
- Open, transparent body
- Representation from all SG stakeholder groups
  - Over 360 member organizations at founding
- Membership open to any materially interested stakeholder organizations
- 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.

SGIP Vision (cont'd)

- SGIP Governing Board
  - Approves and prioritizes the work of the SGIP
  - Coordinates necessary resources (in dialog with SDOs, user groups, and others) to carry out finalized action plans in efficient and effective manner.
- Standing Committees
  - SG Architecture Committee (SGAC)
  - SG Testing and Certification (SGTC)
  - Additional Committees will be created as needed
- Working Groups
  - Cyber Security Coordination Task Group (CSCTG)
  - Domain Expert Working Groups (DEWGs)
- Structure will be refined as appropriate

SGIP Structure

NIST Oversight

Stakeholder Category Members (22)

SGIP Standing Committee Members (2)

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

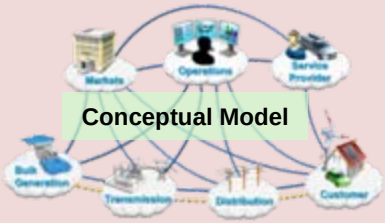
Smart Grid Identified Standards

Priority Action Plans

Use Cases

Requirements

Standards Descriptions



Products (IKB)

NIST National Institute of Standards and Technology

SGIP Stakeholder Categories

1	Appliance and consumer electronics providers
2	Commercial and industrial equipment manufacturers and automation vendors
3	Consumers – Residential, commercial, and industrial
4	Electric transportation industry Stakeholders
5	Electric utility companies – Investor Owned Utilities (IOU)
6	Electric utility companies - Municipal (MUNI)
7	Electric utility companies - Rural Electric Association (REA)
8	Electricity and financial market traders (includes aggregators)
9	Independent power producers
10	Information and communication technologies (ICT) Infrastructure and Service Providers
11	Information technology (IT) application developers and integrators
12	Power equipment manufacturers and vendors
13	Professional societies, users groups, and industry consortia
14	R&D organizations and academia
15	Relevant Federal Government Agencies
16	Renewable Power Producers
17	Retail Service Providers
18	Standard and specification development organizations (SDOs)
19	State and local regulators
20	Testing and Certification Vendors
21	Transmission Operators and Independent System Operators
22	Venture Capital

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
- NIST determined which require most urgent resolution and selected top 15 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
- The Smart Grip Interoperability Panel will eventually guide and oversee progress on PAPs and development of new PAPs.

Priority Action Plans (PAPs)

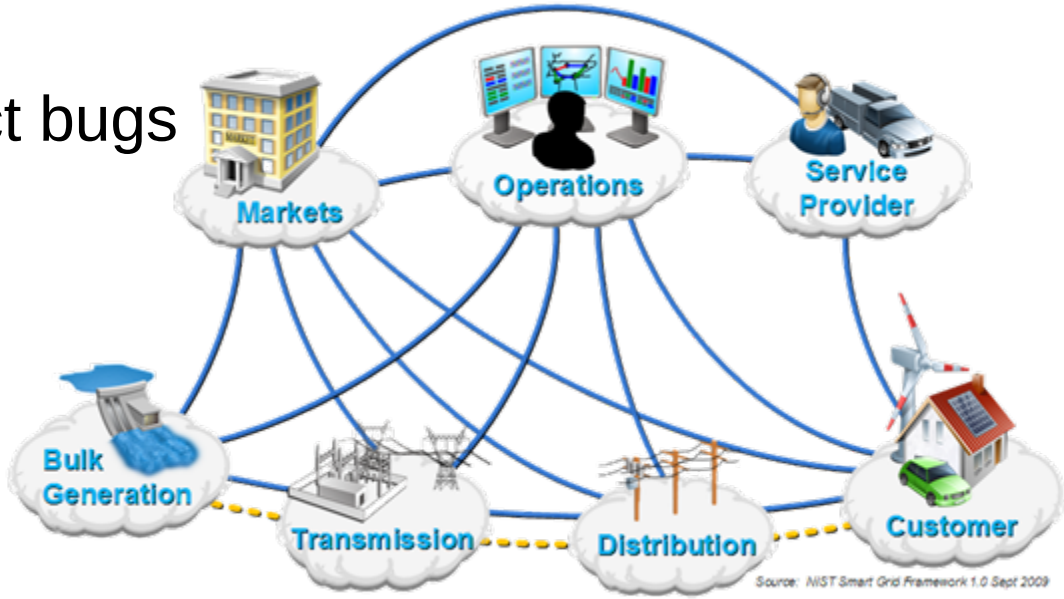
Priority Action Plans
Smart meter upgradeability standard (PAP 00)
Develop common specification for price and product definition (PAP 03)
Develop common scheduling communication for energy transactions (PAP 04)
Develop common information model (CIM) for distribution grid management (PAP 08)
Standard demand response signals (PAP 09)
Standard for energy use information (PAP 10)
DNP3 Mapping to IEC 61850 Objects (PAP 12)
Standard meter data profiles (PAP 05)

Priority Action Plans (PAPs) (cont'd)

Priority Action Plans (continued)
Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronization (PAP 13)
Transmission and distribution power systems model mapping (PAP 14)
Guidelines for use of IP protocol suite in the Smart Grid (PAP 01)
Guidelines for the use of wireless communications (PAP 02)
Energy storage interconnection guidelines (PAP 07)
Interoperability standards to support plug-in electric vehicles (PAP 11)
Harmonize power line carrier standards for appliance communications in the home (PAP 15)

The Need For Conformance Testing

- Must work end to end
- Prime focus on inter-domain operations
- Some companies asking for intra-domain testing
- Standards contain many options
- Standards may contain optional ways to support a feature
- Testing helps correct bugs
- Feedback to SDOs

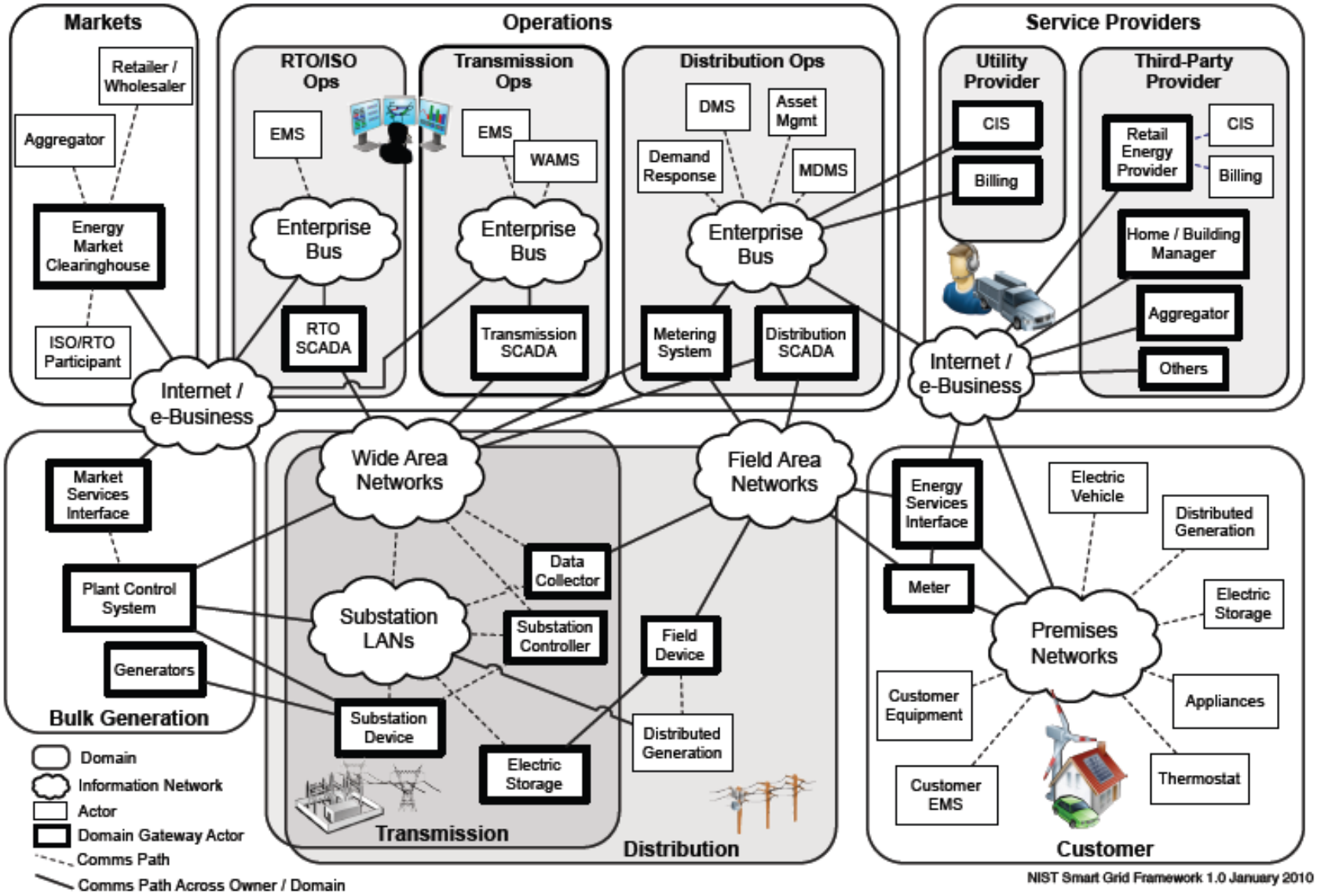


NIST National Institute of Standards and Technology

Conformance Testing Framework

- Leverage Standards Testing Programs Within Current SDOs
  - Not interested in duplicating programs
- Need to Identify Existing Gaps
  - Some SDOs do not write test cases
  - Many SDOs do not define overall test programs
- What Type of Testing
  - Range of testing options from vendor self test to independent third party
  - Validation Process to Confirm Test Cases
  - Protocol Testing
  - Inter-Operability Testing
  - Closer coupling with standards development

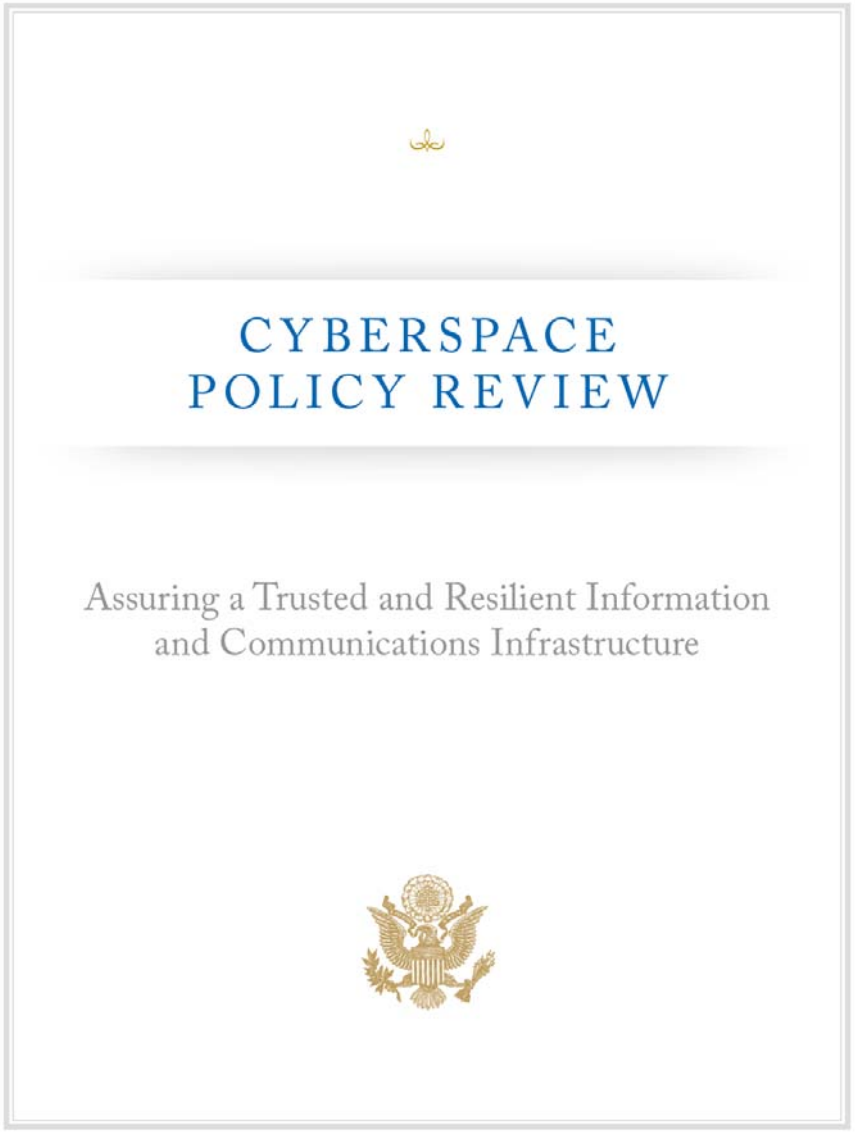
NIST Smart Grid Conceptual Model



NIST Smart Grid Framework 1.0 January 2010

NIST National Institute of Standards and Technology

President's Cyberspace Policy Review



…as the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks.

NIST National Institute of Standards and Technology

Current Grid Environment

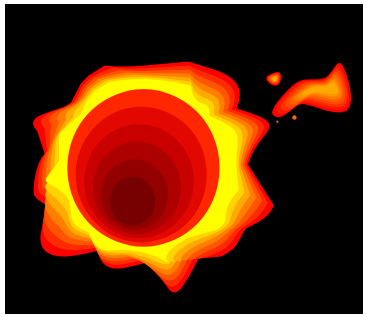
- Legacy SCADA systems
- “Security by Obscurity”
- Limited cyber security controls currently in place
  - Specified for specific domains – bulk power distribution, metering
- Vulnerabilities might allow an attacker to
  - Penetrate a network,
  - Gain access to control software, or
  - Alter load conditions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

Smart Grid: An Opportunity

- Modernization provides an opportunity to improve security of the Grid
- Integration of new IT and networking technologies brings both new risks as well as an array of security standards, processes, and tools
- Architecture is key: security must be designed in – it cannot be added on later

Threats to the Grid

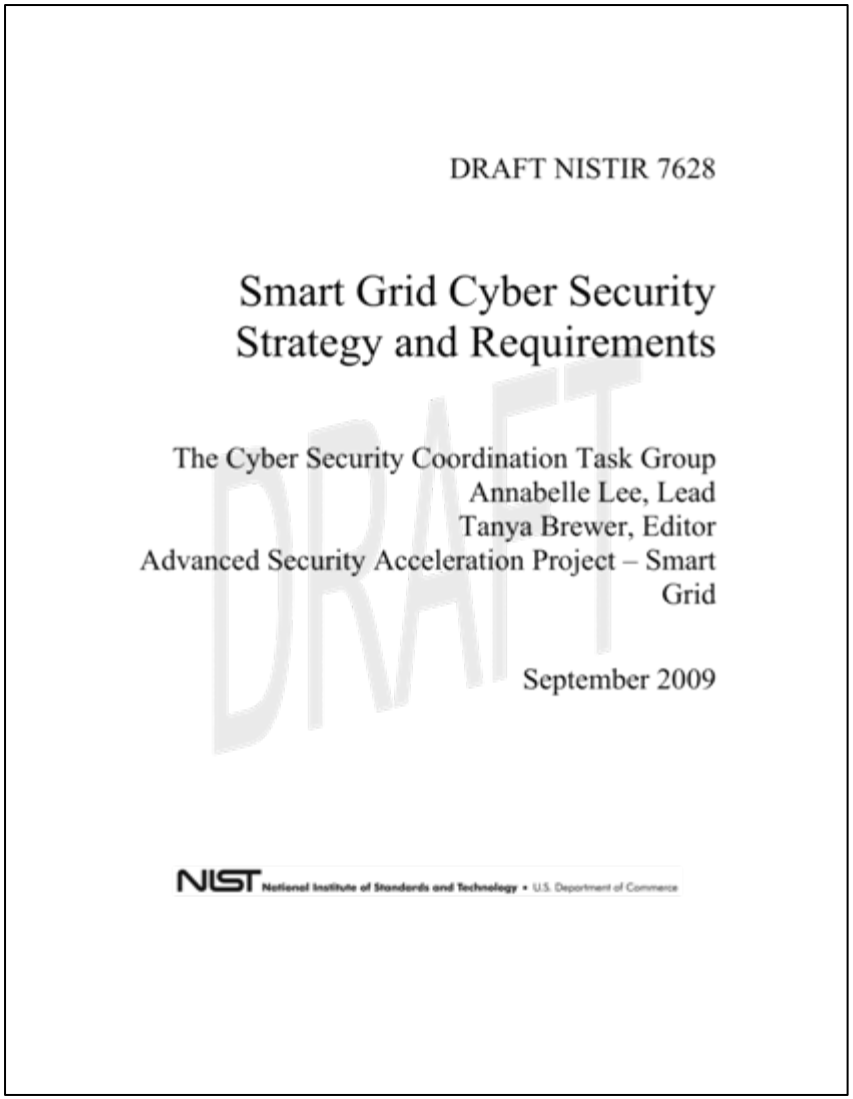
- Deliberate attacks
  - Disgruntled employees
  - Industrial espionage
  - Unfriendly states
  - Terrorists
  - EMP
- Inadvertent threats
  - Equipment failures
  - User errors
- Natural phenomena
  - Disasters
  - Solar activity



New Risks

- Greater complexity increases exposure to potential attackers and unintentional errors
- Linked networks introduce common vulnerabilities
- “Denial of Service” – type attacks
- Increased number of entry points and paths
- Compromise of data confidentiality or customer privacy
- Disruption of IT equipment by EM Pulse, EMI, and Geomagnetically Induced Currents

Smart Grid Cyber Security Strategy



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
National Institute of Standards and Technology

Further Information

- Web portal: http://www.nist.gov/smartgrid
- Contact:
  - Annabelle Lee, Senior Cyber Security Strategist
  - Email: annabelle.lee@nist.gov
  - Telephone: 301.975.8897

NIST
National Institute of Standards and Technology