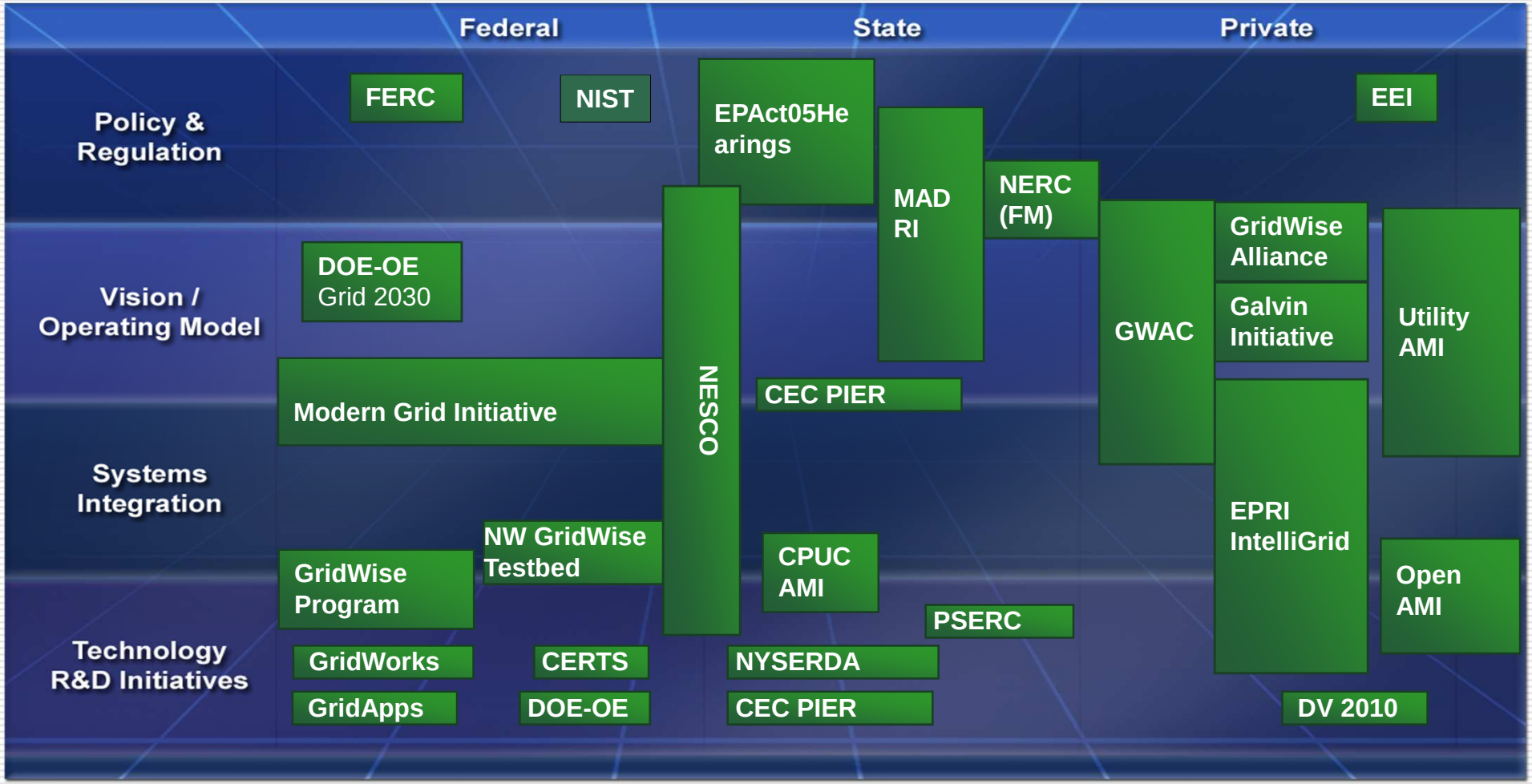
Update on NIST Smart Grid Cybersecurity Activities

Sandy Bacik, CISSP, CISM, ISSMP, CGEIT
Principal Consultant, EnerNex
sandy.bacik@enernex.com

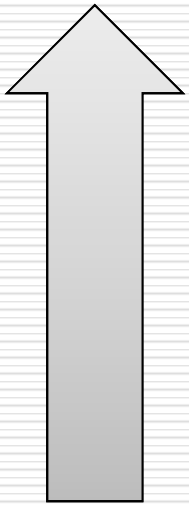
Smart Grid Developers



NIST's Role

Government Roles in Smart Grid

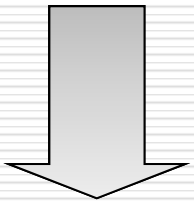
Federal



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

Roles for the Smart Grid

- Department of Energy (DOE) is the lead agency for U.S. Government for Smart Grid
  - $3.4 billion of ARRA-funded Smart Grid Investment Grants
  - Smart Grid Task Force – DOE, NIST, FERC, FCC, EPA, ITA, DHS, …
- NIST coordinates and accelerates development of standards by private sector SDOs
- Federal Energy Regulatory Commission initiates rulemaking
- State Public Utilities Commissions (California, Texas, …)

Energy Independence and Security Act

- In the Energy Independence and Security Act (EISA) of 2007
  - Congress established the development of a Smart Grid as a national policy goal

- Under EISA, NIST is directed to
  - "Coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems"
  - Maintain the reliability and security of the electricity infrastructure

Energy Independence and Security Act (2)

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

Energy Independence and Security Act (3)

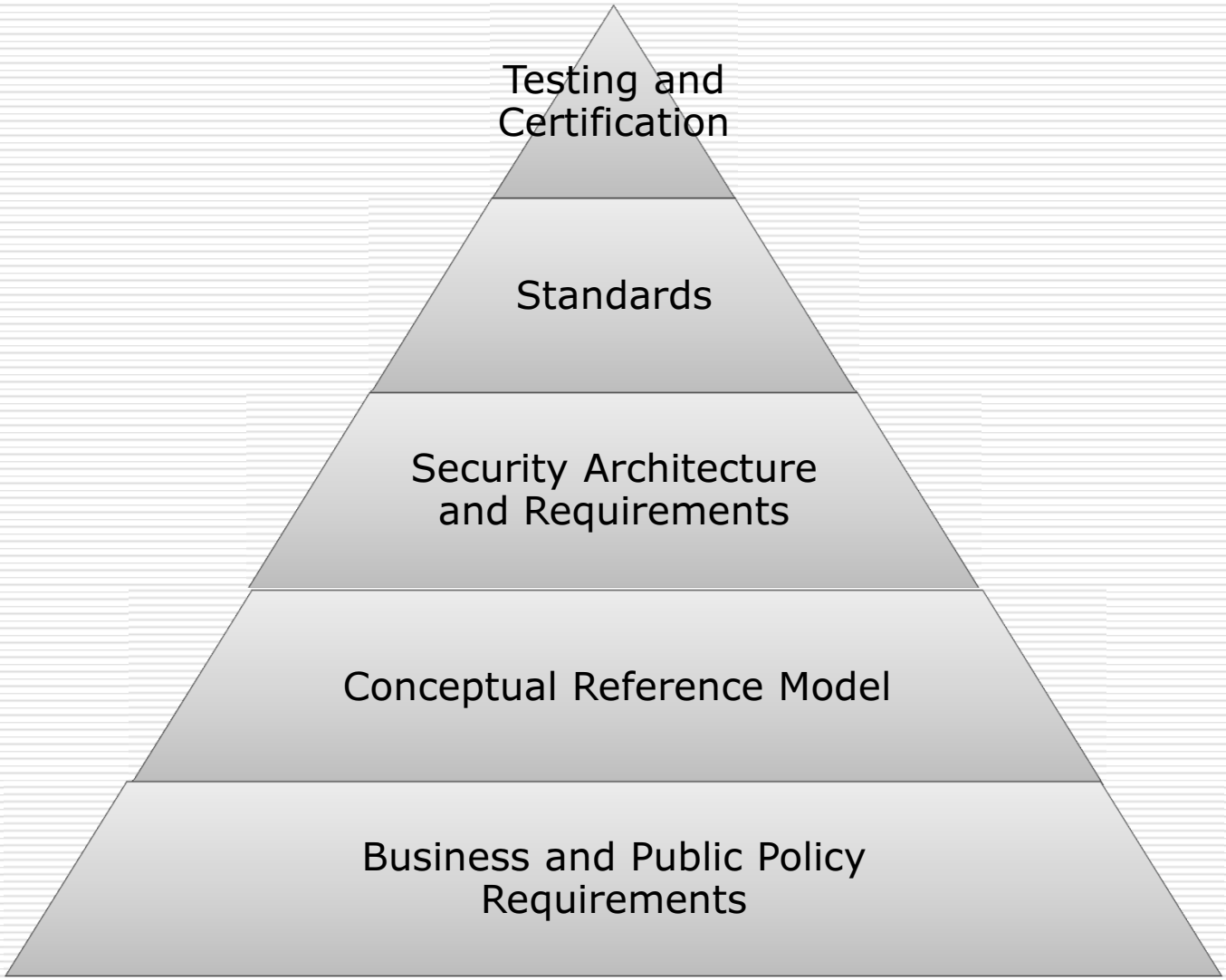
Defines ten national policies for the Smart Grid

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**

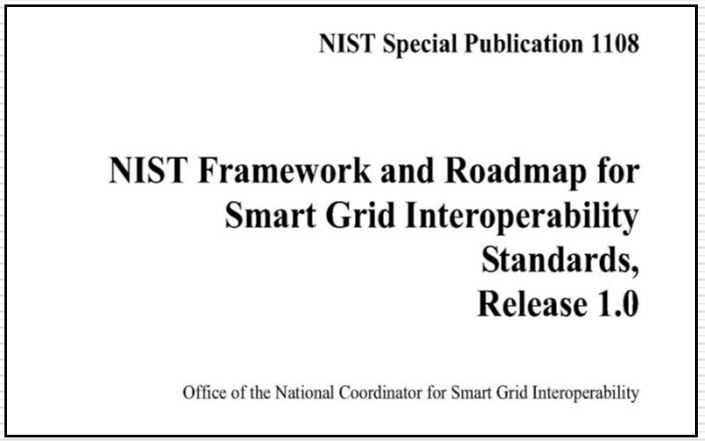
Interoperability Framework



NIST Framework and Roadmap, Release 1.0

- Revised version January 2010
  - Public comments reviewed and addressed
- Smart Grid Vision/Model
- 75 key standards identified
  - IEC, IEEE, …
- 17 Priority Action Plans to fill gaps
- Includes cyber security strategy
  - Companion document, NISTIR 7628 *Guidelines for Smart Grid Cyber Security*

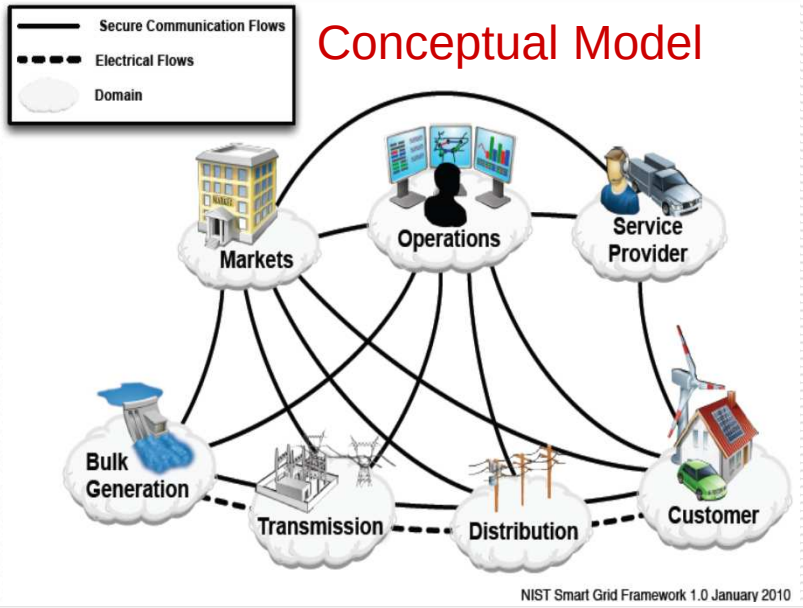
http://www.nist.gov/smartgrid/


NIST Special Publication 1108

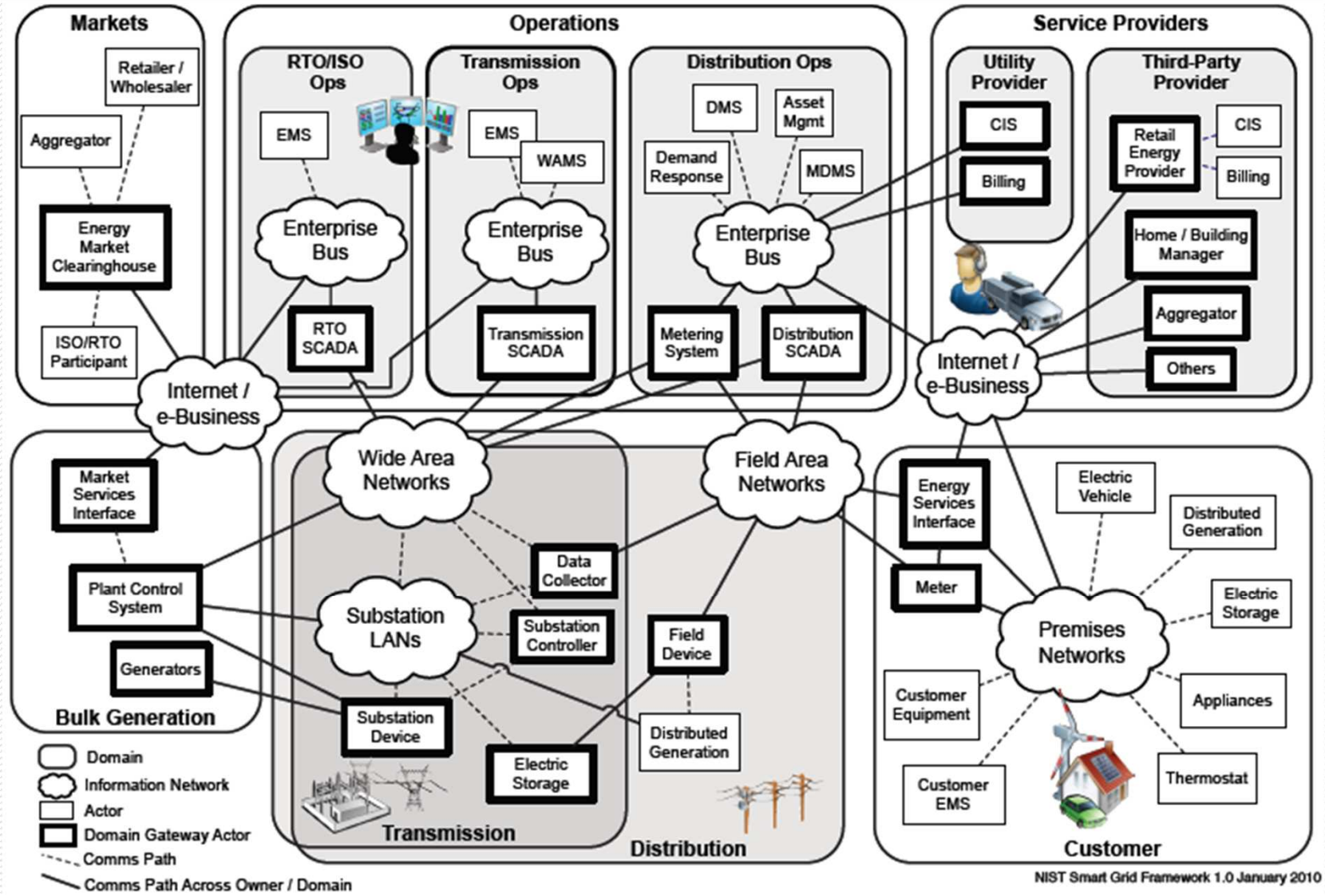
NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

Office of the National Coordinator for Smart Grid Interoperability

Conceptual Model

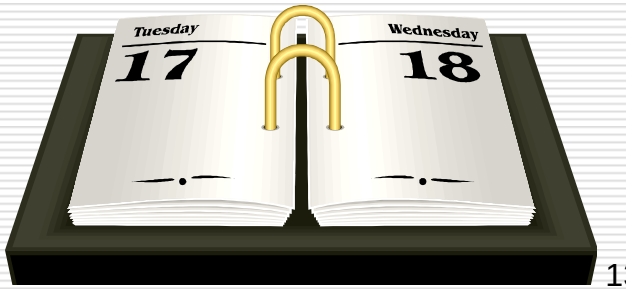


Conceptual Reference Diagram for Smart Grid Information Networks



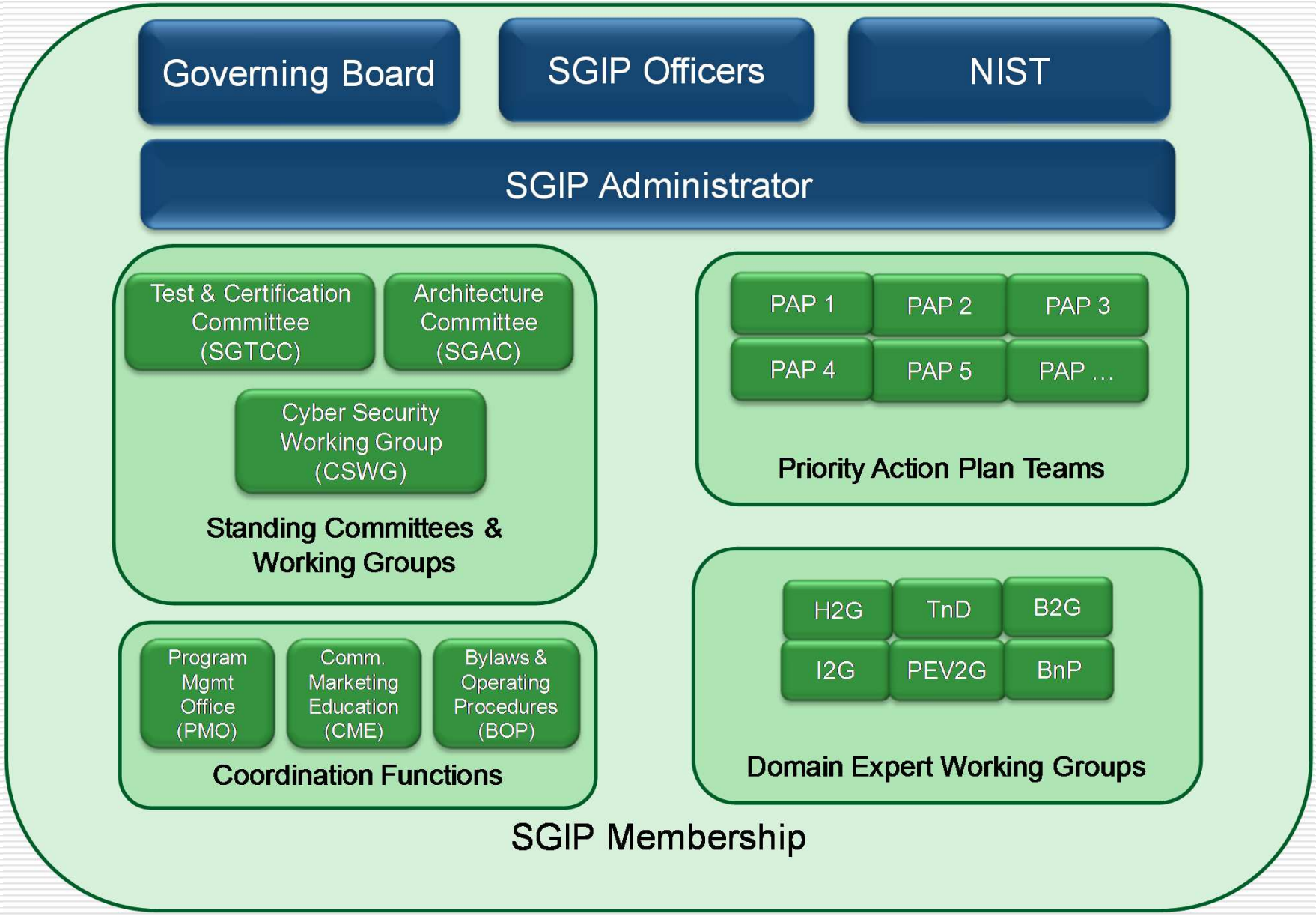
NIST Smart Grid Timeline - Highlights

- 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 NIST holds ***large-scale workshops*** to identify standards
  - Over 1500 participants from a variety of groups
- 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***
- 2010 August
  - CSWG ***Guidelines for Smart Grid Cyber Security*** was released



Smart Grid Interoperability Panel (SGIP)

SGIP Organization and Stakeholders



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 interested stakeholder organizations
- 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 (2)

- 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 Working Group (CSWG)
  - Domain Expert Working Groups (DEWGs)

SGIP Standing Committees

- Smart Grid Architecture Committee (SGAC)
  - Creates and refines SG Conceptual Reference Model
  - Developing Smart Grid Architectural Framework Templates
- Testing and Certification Committee (SGTCC)
  - Creates and maintains the framework for compliance, interoperability and cyber security testing and certification
  - Develops and implements certification criteria by which compliance can be verified through testing of vendor products and services

For More Information

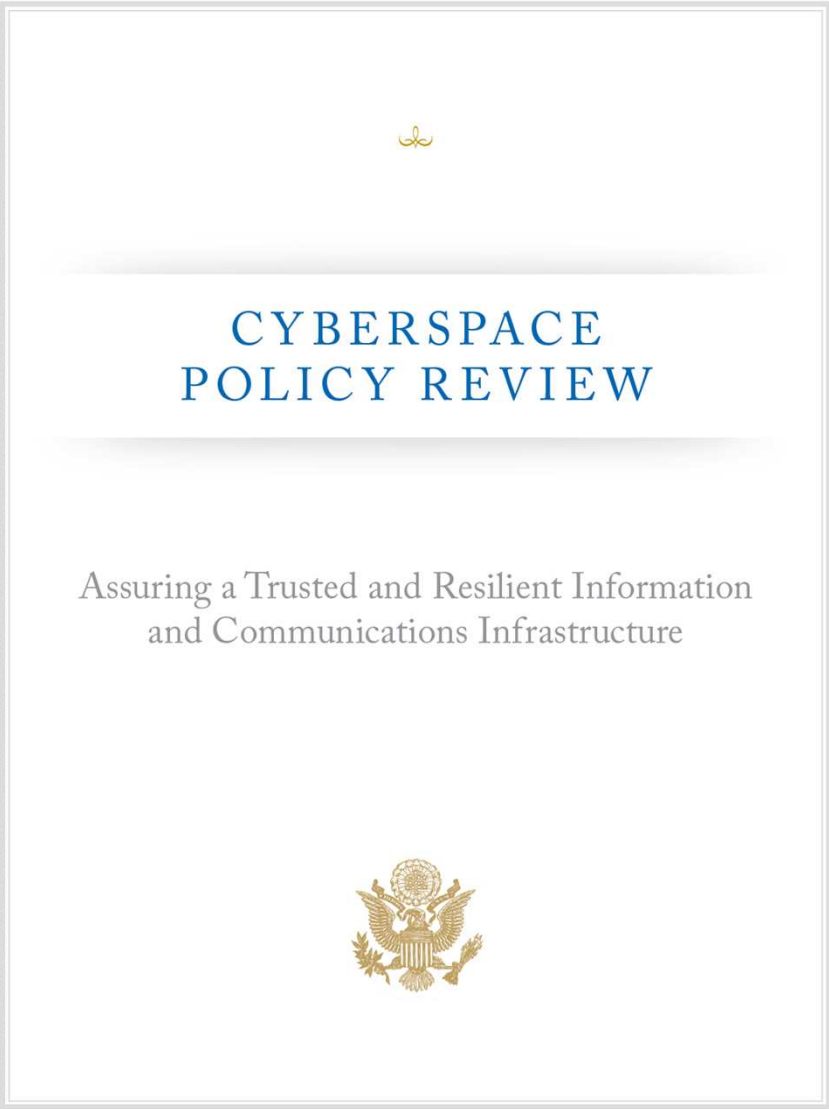
- The *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* (January 2010) can be downloaded at: www.nist.gov/smartgrid/

- The SGIP website is: www.sgipweb.org

- Activities of SGIP committees and working groups can be followed at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIP

Cyber Security Working Group (CSWG)

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.

Current Smart 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
  - 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 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

CSWG

- To address the cross-cutting issue of cyber security
  - NIST established the Cyber Security Coordination Task Group (CSCTG) in March 2009
- Moved under the NIST SGIP as a standing working group and was renamed the Cyber Security Working Group (SGIP–CSWG)
- The CSWG now has more than 500 participants
  - Private sector (including vendors and service providers)
  - Academia
  - Regulatory organizations
  - National research laboratories
  - Federal agencies

CSWG Goals

- Goals
  - Develop an overall cyber security strategy for the Smart Grid that includes a risk mitigation strategy to ensure interoperability of solutions across different domains/components of the infrastructure
    - The cyber security strategy needs to address
      - Prevention
      - Detection
      - Response
      - Recovery
    - Strategy includes the development of a risk mitigation strategy
  - Implementation of a cyber security strategy requires
    - Definition and implementation of an overall cyber security risk assessment process for the Smart Grid

CSWG Objectives

The following objectives address the CSWG's primary goal. These objectives may change as more Smart Grid implementations occur and Smart Grid technologies further develop.

1. Identifying Smart Grid specific problems and issues that currently do not have solutions.
2. Creating a logical reference model of the Smart Grid.
3. Identifying inherent privacy risk areas and feasible ways in which those risks might be mitigated.
4. Developing a conformity assessment program for security requirements in coordination with activities of the SGIP's Smart Grid Testing and Certification Committee (SGTCC).

CWSG Subgroups and Leads

- **AMI Security**
  - Darren Highfill, Ed Beroset, Sandy Bacik
- **Architecture Group**
  - Sandy Bacik
- **Design Principles Group**
  - Daniel Thanos, Annabelle Lee
- **High Level Requirements Group**
  - Dave Dalva, Victoria Yan
- **Privacy Group**
  - Rebecca Herold
- **R & D Group**
  - Isaac Ghansah, Daniel Thanos
- **Standards Group**
  - Frances Cleveland
  - Assistance from Sandy Bacik, Vicky Yan
- **Testing & Certification**
  - Nelson Hastings, Sandy Bacik

NISTIR 7628
Guidelines for Smart Grid Cyber Security

Guidelines for Smart Grid Cyber Security

- NIST Interagency Report 7628 v1.0 posted August 2010
  - Development of the document lead by NIST
  - Represents significant coordination among
    - Federal agencies
    - Private sector
    - Regulators
    - Academics
  - Document includes material that will be used in selecting and modifying security requirements

NISTIR 7628 – What it IS and IS NOT

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

NISTIR 7628 Content

The NISTIR includes the following

- Executive Summary
- Overview and document organization
- Chapter 1 - Cyber Security Strategy
- Chapter 2 – Logical Architecture and Interfaces of the Smart Grid
- Chapter 3 – High-Level Security Requirements
- Chapter 4 – Cryptography and Key Management

NISTIR 7628 Content (2)

- Chapter 5 – Privacy and the Smart Grid
- Chapter 6 – Vulnerability Classes
- Chapter 7 – Bottom-Up Security Analysis of the Smart Grid
- Chapter 8 – Research and Development Themes for Cyber Security in the Smart Grid
- Chapter 9 – Overview of the Standards Review
- Chapter 10 – Key Power System Use Cases for Security Requirements
- Appendices A - J

Roadmap - Activities

- Face to Face Meetings
  - Provide an opportunity for the CSWG members to interact and meet
  - Have technical working sessions on specific areas of the NISTIR 7628 and other documents
  - Review new material for subgroups
  - Plan future activities for the CSWG
  - Coordinate tasks that fall under multiple sub-groups

- Coordination with other Federal Agencies and other Smart Grid groups
  - Goal of inter-agency coordination
    - Promote communication among participants of the various Smart Grid cyber security programs/projects across the federal government
  - Objective is to keep all individuals informed

The Way Forward…

- Activities…
  - Continued Outreach and education
    - Universities
    - Private sector organizations
    - Standards bodies
    - Other organizations
  - Coordination with the other organizations within the SGIP
    - SGIP Governing Board (GB)
    - SG Architecture Committee (SGAC)
    - SG Test and Certification Committee (SGTCC)
    - Priority Action Plan (PAP) working groups
    - SGIP Program Management Office (PMO)
  - Participation in the development of a cyber security conformity assessment strategy

The Way Forward (2)…

- Future activities…
  - Further development of R&D themes
  - Cryptographic and key management issues
  - Expand privacy efforts
  - New subgroups formed: AMI Security, Design Principles, and Testing & Certification
  - Participation in a DOE Office of Electricity Delivery and Energy Reliability (OE) public-private initiative to develop a harmonized energy sector enterprise-wide risk management process
  - Expand coordination with the SGTCC to develop guidance and recommendations on Smart Grid conformance, interoperability and cybersecurity testing
  - Provide cybersecurity expertise on how best to address cyber-physical threats in coordination with other federal agencies and industry groups

How to Participate in CSWG

- NIST Smart Grid portal:
  - http://nist.gov/smartgrid
- Cyber Security Working Group
  - Lead: Marianne Swanson (marianne.swanson@nist.gov)
  - NIST Support: Tanya Brewer (tanya.brewer@nist.gov)
- Cyber Security Twiki site
  - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG