National Institute of Standards and Technology Smart Grid Cybersecurity

Vicky Yan Pillitteri
Advisor for Information Systems Security
SGIP SGCC Chair
Victoria.yan@nist.gov

The National Institute of Standards and Technology (NIST)

- NIST is an non-regulatory agency within the U.S. Department of Commerce

- Mission: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that embrace economical security and improve our quality of life

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

Executive Order 13636, Improving Critical Infrastructure Cybersecurity

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

- NIST is directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure

- This Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment process, workshops, and other means of engagement.

The Cybersecurity Framework

For the Cybersecurity Framework to meet the requirements of the Executive Order, it must:

- include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.
- provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.
- identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations able technical innovation and account for organizational differences include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

"Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0" was released on February 13, 2014 and is available at: http://www.nist.gov/cyberframework/index.cfm

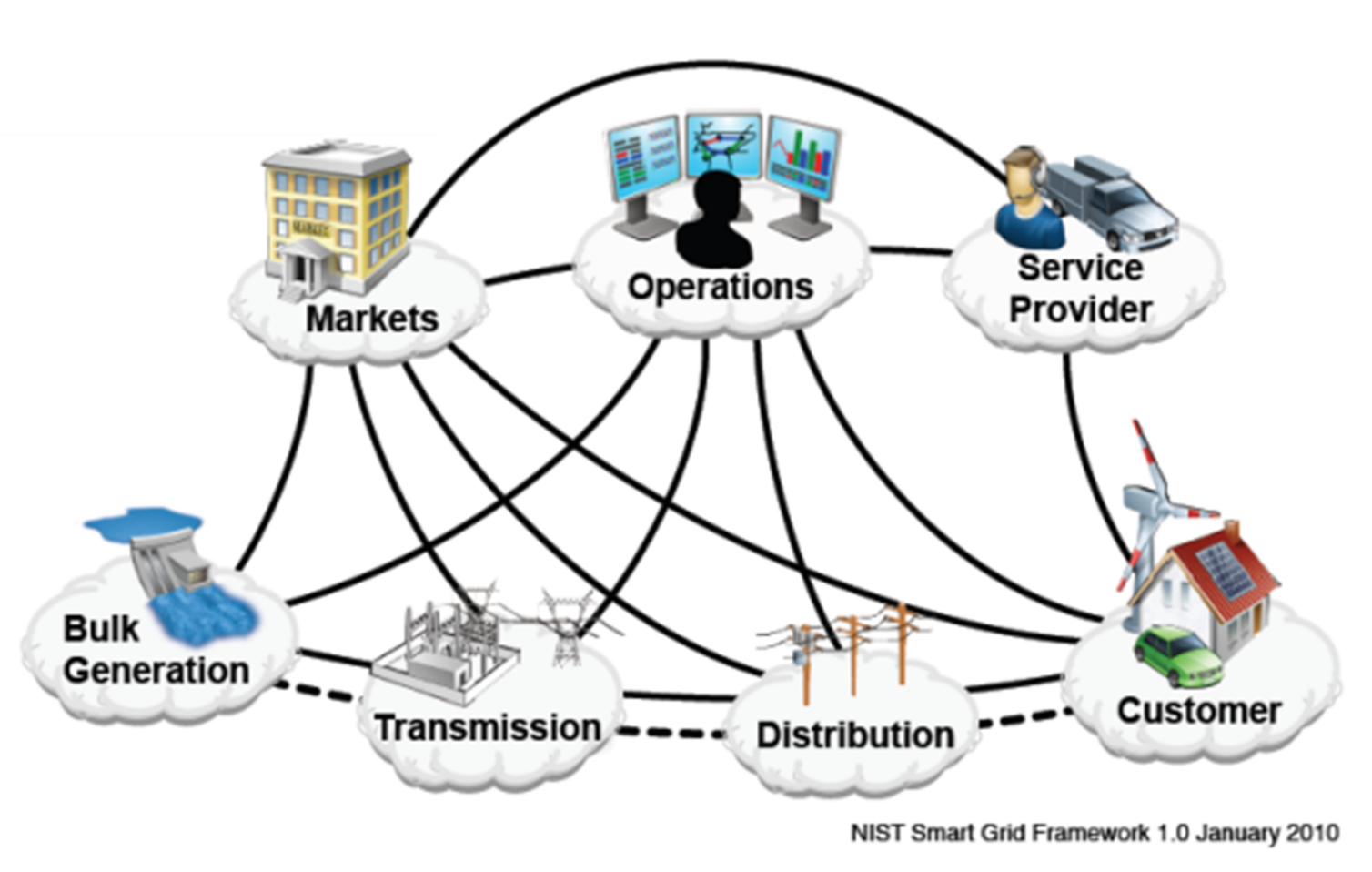
NIST's Role in the Smart Grid

- 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**

Smart Grid Cybersecurity

- Cybersecurity is recognized as a critical, cross-cutting issue that must be addressed in all standards developed for Smart Grid
- The cybersecurity strategy for Smart Grid must be a continuing work in progress so new and changing requirements are anticipated and addressed
- There are also emerging privacy issues related to consumer adoption of Smart Grid technologies

Smart Grid Cybersecurity is critical across all domains



The Impact of Smart Grid Cybersecurity

- Interoperable standards for the Smart Grid with **security "baked in,"** providing long term savings in resources to prevent a need to retrofit security into products
- **Standardized foundation** for cybersecurity of cloud applications
- **Acceleration and coordination** of research and practices to aid in mitigating emerging cyber-physical vulnerabilities
- **Lead/facilitate standardization** of a set of AMI security requirements
- **Privacy protections** for owners/operators of plug-in electric vehicles and occupants of buildings with AMI meters (expected to be hundreds of millions in U.S. alone