


NIST Smart Grid Program

## Smart Grid Cybersecurity Update

**NIST Smart Grid Federal Advisory Committee**  
June 3, 2014

**Vicky Yan Pillitteri**  
[victoria.yan@nist.gov](mailto:victoria.yan@nist.gov)

Computer Security Division, Information Technology Laboratory  
National Institute of Standards and Technology



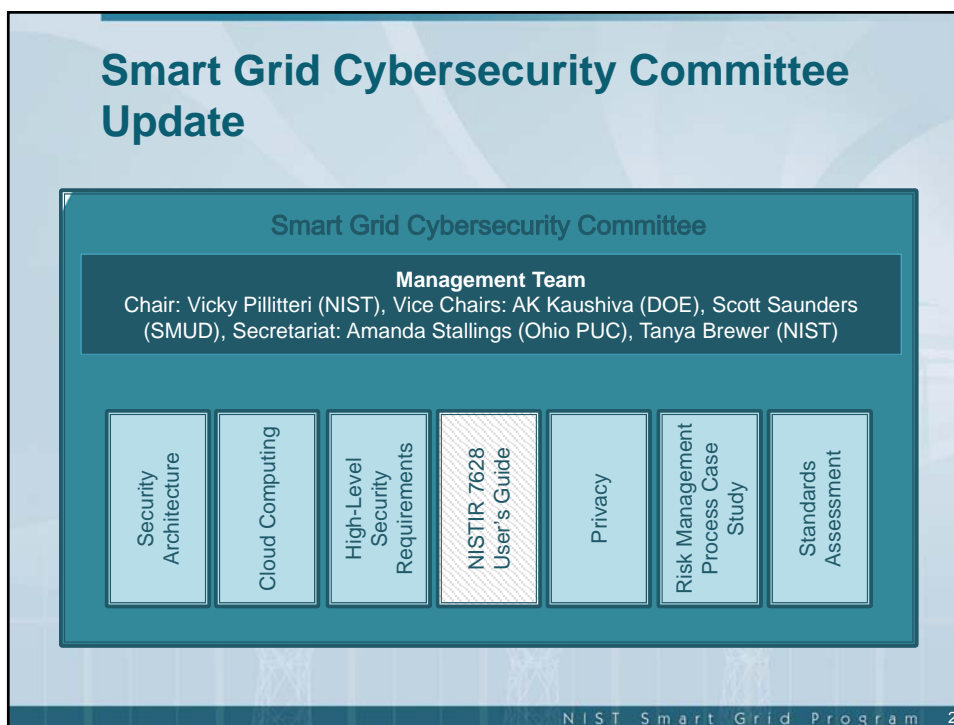
## Smart Grid Cybersecurity Committee Update

**Smart Grid Cybersecurity Committee**

**Management Team**  
Chair: Vicky Pillitteri (NIST), Vice Chairs: AK Kaushiva (DOE), Scott Saunders (SMUD), Secretariat: Amanda Stallings (Ohio PUC), Tanya Brewer (NIST)

Security Architecture	Cloud Computing	High-Level Security Requirements	NISTIR 7628 User's Guide	Privacy	Risk Management Process Case Study	Standards Assessment
-----------------------	-----------------	----------------------------------	--------------------------	---------	------------------------------------	----------------------

NIST Smart Grid Program 2



## Smart Grid Cybersecurity Accomplishments & Planned Activities

### Accomplishments

- Publication of NISTIR 7628 User's Guide (March 2014)
- Submitted comments on CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security interim report
- Hosted webinar on Cybersecurity Framework (April 2014)
- Cybersecurity reviews of smart grid-related standards, guidelines, and documents (ongoing)
- Mapping of NISTIR 7628 High-Level Security Requirements to draft NERC CIP v5 (2013) and Cybersecurity Framework Core (May 2014)

### Planned Activities

- Publication of:
  - Defense in Depth and Breadth White Paper (Summer 2014)
  - Cloud Computing Considerations White Paper (Summer 2014)
  - Risk Management Process Case Study (Summer 2014)
  - NISTIR 7823, Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework (Fall 2014)
  - NISTIR 7628, Rev. 1 (Fall 2014)
- Development of smart grid cybersecurity testbed

NIST Smart Grid Program 3

## Executive Order: 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"*

President Barack Obama  
Executive Order 13636, Feb. 12, 2013

- NIST was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work

NIST Smart Grid Program 4

## Based on the Executive Order, the Cybersecurity Framework 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 to be addressed through future collaboration with particular sectors and standards-developing organizations

NIST Smart Grid Program 5

## The Cybersecurity Framework is for Organizations

- Of any size, in any sector in the critical infrastructure
- That already have a mature cyber risk management and cybersecurity program
- That don't yet have a cyber risk management or cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business or societal threats

NIST Smart Grid Program 6

## How to Use the Cybersecurity Framework

The Framework is designed to complement existing business and cybersecurity operations, and can be used to:

- Understand security status
- Establish / Improve a cybersecurity program
- Communicate cybersecurity requirements with stakeholders, including partners and suppliers
- Identify opportunities for new or revised standards
- Identify tools and technologies to help organizations use the Framework
- Integrate privacy and civil liberties considerations into a cybersecurity program

NIST Smart Grid Program 7

## Energy Sector Implementation Guidance

- Per Section 8 of the Executive Order, Department of Energy is developing sector-specific implementation guidance for the Cybersecurity Framework
- Recognizes existing subsector-specific approaches to cybersecurity such as:
  - North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP)
  - NIST Interagency Report 7628, Guidelines for Smart Grid Cybersecurity
  - Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
- Effort includes strong private industry participation as well as cross-federal agency coordination

NIST Smart Grid Program 8

