Smart Grid and Cyber Security

Annabelle Lee

Senior Cyber Security Strategist

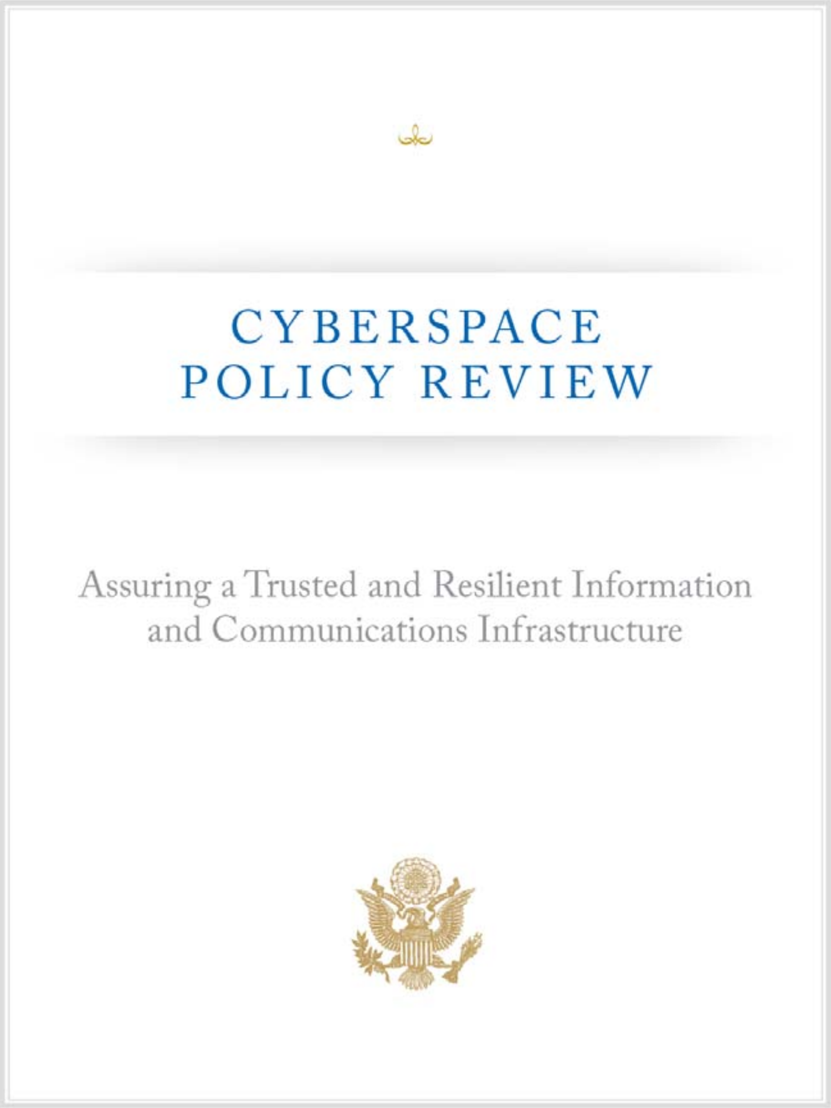
Computer Security Division

National Institute of Standards and Technology

December 10, 2009

NIST
National Institute of Standards and Technology

President’s Cyberspace Policy Review



CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

…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.

Smart Grid Cyber Security Strategy

- Establishment of a Cyber Security Coordination Task Group (CSCTG)
    - Over 270 participants
    - Have established several working groups
        - Vulnerability class analysis
        - Bottom-Up assessment
        - Privacy
        - Standards assessment
        - High level requirements
        - Functional architecture development
        - Research and Development
    - Weekly telecon

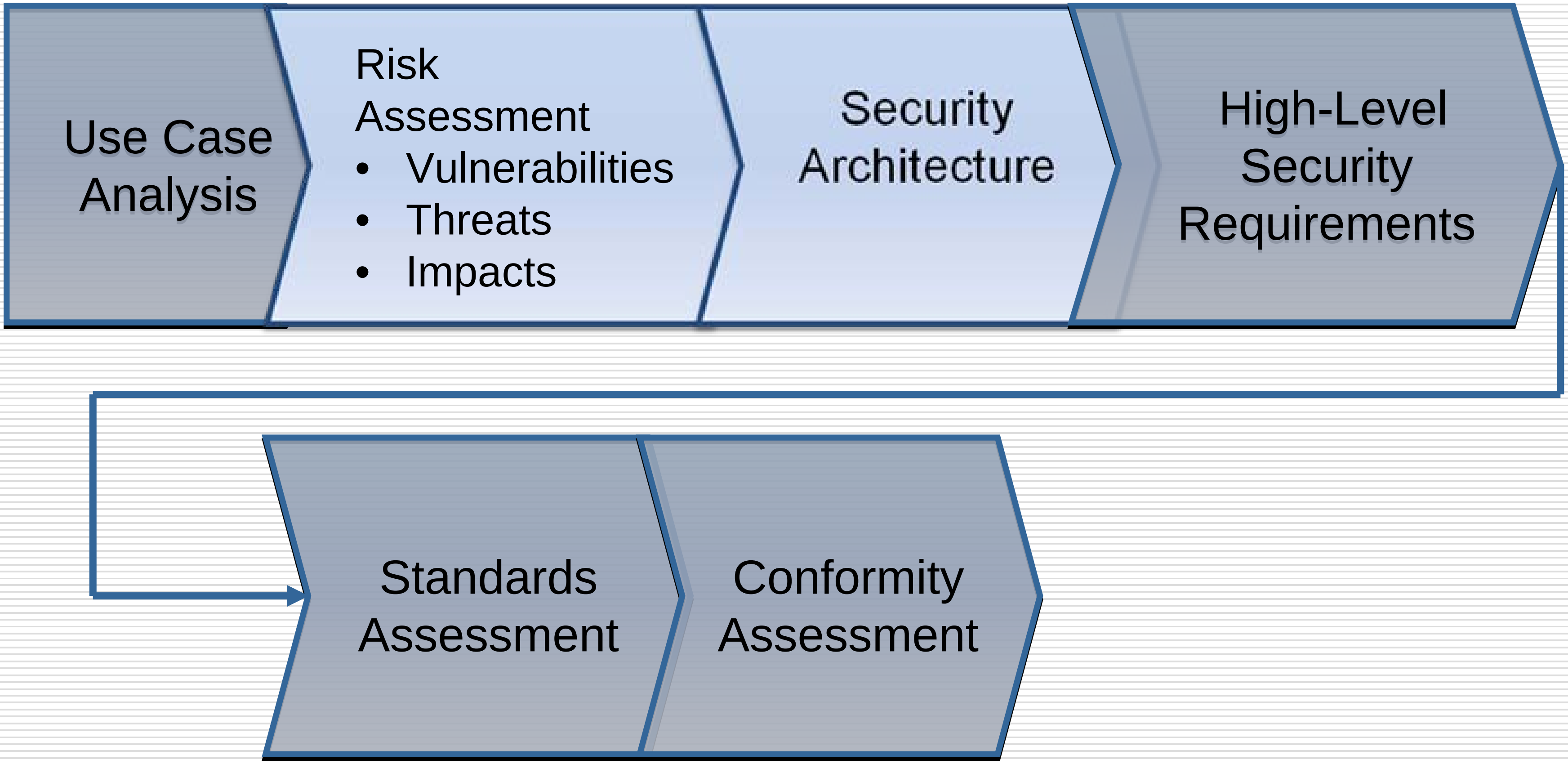
Smart Grid Cyber Security Strategy (2)

- The strategy…
  - Selection of use cases with cyber security considerations
  - Performance of a risk assessment of the Smart GridDevelopment 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

The Way Forward…

- Future activities…
  - Cryptographic and key management
  - Participation in the development of a cyber security conformity assessment strategy
- The overall cyber security strategy for the Smart Grid must address both domain-specific and common risks
  - Understand the threats
  - Identify the missions of the system and impacts
  - Categorize the data and processes to be protected

NIST Cyber Security Coordination Task Group (CSCTG) Work Program



Use Case Analysis

Risk Assessment
- Vulnerabilities
- Threats
- Impacts

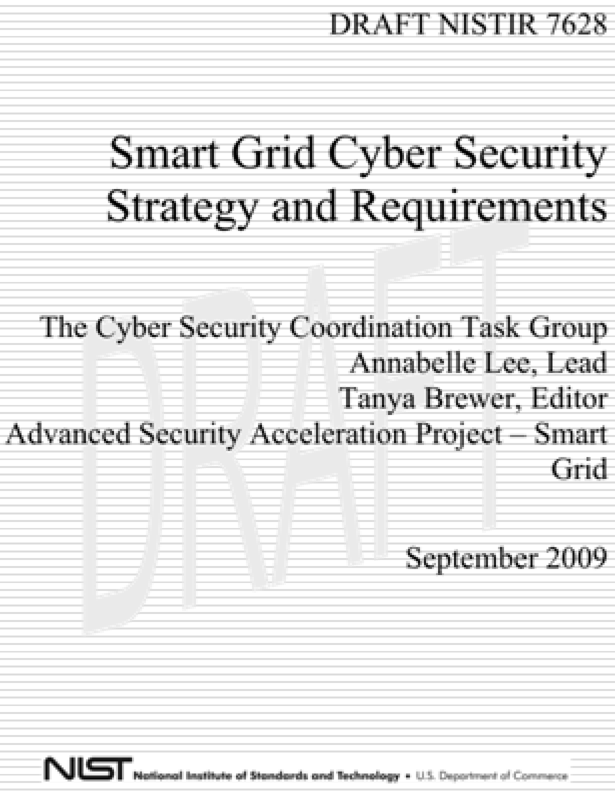
Security Architecture

High-Level Security Requirements

Standards Assessment

Conformity Assessment

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

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

Smart Grid Cyber Security Strategy and Requirements Draft (2)

- Current plan is to publish a second draft at the end of January 2010
  - 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
    - Initial assessment of standards
    - R and D topics
    - Crypto/key management
- Final version planned for spring 2010

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

NISTIR 7628 (2)

- The draft NISTIR includes the following sections (2):
  - Specification of confidentiality, integrity, and availability impact levels (low, moderate, high) for each category
  - 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

NISTIR 7628 (3)

- The draft NISTIR includes the following sections (2):
  - Key power system use cases with security considerations
    - Extracted from several sources
  - Vulnerability categories
    - Aggregation of specific vulnerabilities identified from several sources
  - 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

Working Group Summaries

- General information on each working group: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WorkingGroupInfo
  - Includes weekly telecon day/time and call-in numbers
  - Lists working group leads and email

Vulnerability Class Analysis

- Matt Carpenter, Matt Thomson
- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGVulnerabilities
  - A technical group providing insight and context on vulnerabilities and risk throughout the smart grid
- Current status
  - Focused on vulnerability classes rather than specific vulnerabilities

Vulnerability Class Analysis (2)

- Current status (2)
  - Vulnerability document with a list of vulnerability classes/use case topics is complete
- What's Next?
  - Mapping from *Bottoms Up* work to Vulnerability Classes, to Architecture
    - Review of High-Level Requirements Documents
    - Continuing to provide technical insight and context to vulnerability discussions

Bottom-Up Cyber Security Analysis

- Andrew Wright, Daniel Thanos
- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGBottomUp
- Background...
  - **Bottom-up** analysis of cyber security issues in the evolving Smart Grid
  - Identify some specific problems and issues … but not to perform a gap analysis
  - Intended to complement top-down work:
    - More quickly identify fruitful areas for solution development
    - Provide independent validation of top-down requirements

NIST
National Institute of Standards and Technology

Bottom-Up Cyber Security Analysis (2)

- Current document
  - Two Sections:
    - Evident and specific cyber security problems
      - Dialup modems with minimal security
      - Passwords shared amongst IEDs and personnel
    - Non-specific cyber security issues
      - Patch management
      - IDS for power equipment
- Direction
  - Build a “design considerations” section:
    - Issues to think about in design
    - Not a list of requirements or solutions
    - Not something that can be complied with
      - Event management and event response
      - User authentication
      - Crypto/key management

Privacy

- Gal Shpantzer, Rebecca Herold
- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy
- Mission: Identify and describe privacy concerns within the Smart Grid and opportunities for their mitigation. The group strives to identify privacy expectations and practices with regard to the Smart Grid by:
  - Identifying potential privacy problems and encouraging the use of relevant existing fair information practices

Privacy (2)

- Mission (2)
  - Recommend coordination of activities among relevant local, state, and federal agencies regarding Smart Grid privacy related issues
  - Providing information and considerations to organizations developing privacy policies and practices that promote and protect the interest of Smart Grid consumers and organizations
- Current Status
  - Performed a high-level privacy impact assessment (PIA), a portion of which comprised the privacy chapter within the first draft of NISTIR 7628
  - Identified potential privacy concerns within Smart Grid
  - Identifying how existing widely recognized privacy principles and fair information practices may apply to the Smart Grid

Privacy (2)

- Current status (2)
  - Discussing the potential benefits of privacy certification for organizations that are involved with the Smart Grid
  - Identifying existing laws, regulations and standards that apply to Smart Grid data
  - Identifying and reviewing state-level Smart Grid privacy activities
  - Working on the privacy chapter for the second draft of NISTIR 7628

Standards Assessment

- Ramesh Reddi http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGStandards
- Mission
  - Identify and assess the cyber security related standards that are commonly used smart grid applications
- Current Status
  - Identified 46 cyber security related standards

Standards Assessment (2)

- Current status (2)
  - Created a template with attributes including DHS catalog for security control type and OSI layers.
  - Assessment of these identified standards is in process
- Next steps
  - Complete the current assessment process
  - Categorize the standards into groups based on the attributes that are covered
  - Develop a harmonization methodology

Standards Assessment (3)

- Standards being considered from these organizations
  - IEC, IEEE, NIST, W3c, NERC, ISO/IEC, IETF …
- Issues/considerations
  - Availability of some of these identified standards for assessment purposes
  - Need of requirements that are being developed by other subgroups
- Currently benchmarking to DHS catalog security control families

High Level Requirements

- Annabelle Lee, Tom Overman
- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGHighLevelRequirements
- Gathering various high level requirements for the Smart Grid
- Group goals
  - Develop set of security requirements for the Smart Grid
    - Utilizing material developed by the other working groups
  - Evaluating the entire Smart Grid – from end-to-end

High Level Requirements (2)

- Current activities
  - Refining logical interface categories and constraints table
    - Will be basis for identifying and tailoring security requirements
  - Identifying impact levels for confidentiality, integrity and availability for each interface category
  - Reviewing and revising FERC 4+2 interface diagrams
  - Identifying common security controls from DHS Catalog of Security Controls

High Level Requirements (3)

- Next steps
  - Review and revise common security controls, as required
  - Identify and tailor technical controls for interface categories
  - Identify power system controls that may be used to address the requirements
  - Review by other CSCTG working groups
- Issues/considerations
  - Ensuring that all three sectors, IT, telecom, and electric concur on the requirements

Functional Architecture Development

- Justin Searle and Sandy Bacik and cast of dozens
- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGArchi
- Provide conceptual, physical, and functional diagrams
- Documents are posted for questions in talking to vendors, merging the various smart grid domains into a single drawing
- Group Goals
  - Create a reference architecture for Smart Grid

NIST
National Institute of Standards and Technology

Functional Architecture Development (2)

- Group Goals (2)
  - Create physical architectural diagrams showing major variants of typical deployments
  - Update NIST's conceptual (cloud) diagrams and logical FERC 4+2 diagrams
  - Create a common look and feel to all three sets of diagrams
  - Identify major interfaces and data flows across all three sets of diagrams
- Current Progress
  - Created spreadsheet templates to collect and organize information for AMI and HAN

Functional Architecture Development (3)

- Current Progress (2)
  - Started merging all FERC 4+2 diagrams into a single monolithic diagram
  - Started physical diagrams for AMI and HAN
- Timeframes
  - Complete a rough draft of the functional architecture for the January 2010 NISTIR
  - Start working on a security architecture in January 2010
  - Security architecture to be included in the spring 2010 document

Research and Development

- Carl Gunter and Jessica Ascough and
- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGRandD
- Identify research and development needs and ideas as they are identified within the work of the CSCTG
- Will develop an R&D agenda to include both short term (applied research) and long term (basic research) topics

How to Participate in CSCTG

- 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

NIST
National Institute of Standards and Technology