

---

# NIST and the Smart Grid

---

NISTIR 7628, *Guidelines for Smart Grid Cyber Security*

National Institute of Standards and Technology

U.S. Department of Commerce

September 28, 2010



# Agenda Day 1

---

- 10:00 AM SGIP Cyber Security Working Group Welcome  
– Marianne Swanson
- 10:15 AM NIST Smart Grid Interoperability Panel  
Overview – Marianne Swanson
- 10:30 AM DOE Threat Briefing – Mark Enstrom
- 11:00 AM CSWG Overview – Marianne Swanson
- ❑ The CSWG's focus and role
  - ❑ The sub-groups
- 11:30 AM The NIST Interagency Report 7628 – CSWG  
Staff
- ❑ Security Architecture
  - ❑ High-level security requirements
- 12:00 PM Lunch
-

# Agenda Day 1

---

- 1:00 PM The NIST Interagency Report 7628 (Continued)  
– CSWG Staff
- Cryptography and Key Management
  - Vulnerability Classes
  - Bottom-Up Security Analysis
  - Research and Development
  - Standards Review
- 3:30 PM Day 1 Wrap-up
- 4:00 PM Adjourn

---

# **NISTIR 7628, *Guidelines to Smart Grid Cyber Security***

Cryptography and Key Management,  
Vulnerability Classes, Bottom-Up Security  
Analysis, Research & Development, and  
Standards Review

---

# CSWG Cryptography and Key Management Group

Leads:

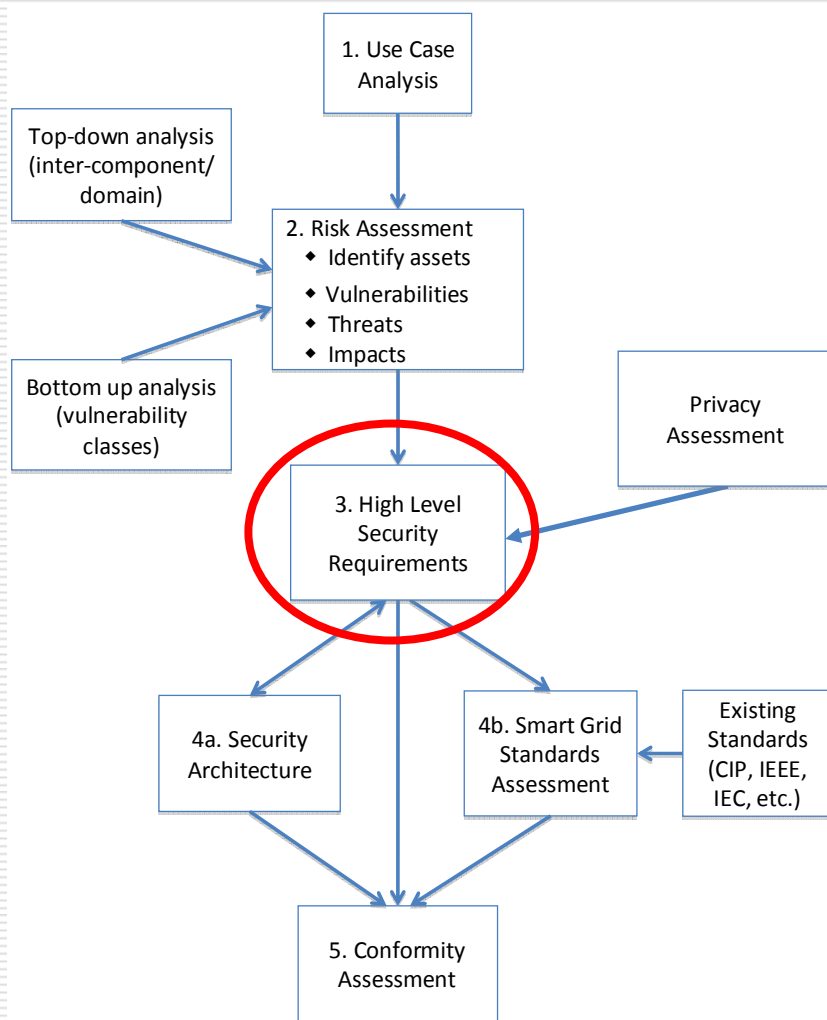
Daniel Thanos ([daniel.thanos@ge.com](mailto:daniel.thanos@ge.com))

Douglas Biggs ([dbiggs@infogard.com](mailto:dbiggs@infogard.com))

Tony Metke ([tony.metke@motorola.com](mailto:tony.metke@motorola.com))

Twiki: [http://collaborate.nist.gov/twiki-  
sggrid/bin/view/SmartGrid/CSCTGCrypto](http://collaborate.nist.gov/twiki-<br/>sggrid/bin/view/SmartGrid/CSCTGCrypto)

# Cryptography and Key Management



- Identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.

# Crypto Sub-Group Scope/Mission

---

- Identification and documentation of
  - General cryptography and key management issues in Smart Grid
  - Technical cryptography and key management issues in specific Smart Grid systems
  - Specifying a NIST approved cipher suite to be used for Smart Grid systems
- Design considerations for key management systems and encryption to be used in Smart Grid
- Key management system requirements aligned to the impact levels specified in the High Level requirements
- Analysis of Smart Grid standards that make use of cryptography
  - Use of existing open cryptography and key management system standards for use in Smart Grid

# CSWG Position on Cryptography

---

- All of the cryptography and other security functions (e.g., hashes, RNGs, etc.) that are required for use in Smart Grid shall be FIPS approved or allowed for use in FIPS modes.
  
- During the development of updated versions, a liaison shall be appointed to coordinate with NIST's Cryptographic Technology Group to ensure that any new algorithms and/or security functions are FIPS approved or allowed and not scheduled to be withdrawn.

# CSWG Position on Cryptography (2)

---

- Standards and systems that take exception to this position on sound technical grounds and are potentially equally secure.
  
- CSWG will consider these alternatives based on submitted technical analysis that explains why the existing NIST recommended or FIPS approved or allowed cryptography suite could not be used.
  - If the submitted technical analysis is sound, these other algorithms, modes, or any relevant crypto primitives will be submitted to NIST to be evaluated for approval for use in Smart Grid systems.

# Crypto Chapter Content

---

- Assumes some level of cryptography knowledge is assumed (i.e. not a tutorial or general education document)
  
- Meant to be used as a guiding framework and not as a standard of any type to be adhered to
  - Can be used in the development of more technically defined standards for specific devices and systems
  
- Design considerations meant to act as guidance towards designing necessary solutions
  - Stops short of specific designs or being prescriptive as innovation is needed from industry

# Crypto Chapter Content (2)

---

- Some problems are
  - General in nature and others very technical and specific
  - Immediate and others will emerge as the Smart Grid evolves
  
- Key management systems and their associated problems and benefits are discussed
  - Strong focus on PKI, other alternatives will require more exploration in future

# Crypto Chapter Content (3)

---

- Problems
  - General constraining issues (e.g. CPU, bandwidth, etc.) found in Smart Grid systems and communications
  - General cryptography issues (e.g. entropy, cipher suites, key management, etc.) for Smart Grid
  - System specific issues
- Design Considerations and Solutions
  - General design considerations (e.g. technique selection, RNG, cryptography modules, etc.)
  - Key management systems for Smart Grid (e.g. PKI and symmetric systems)
- NISTIR high level security requirements
  - Cipher suite for Smart Grid
  - KMS (Key Management System) attributes and requirements for high-level requirements impact levels

# Future Plans

---

- Further development of design considerations
- Evaluation and mapping existing best practices and standards to fulfill KMS requirements
- General evaluation of standards as required by CSWG and broader SGIP groups (e.g., PAPs, Test and certification, Standards group)
- General evaluation of NIST standards that may have impact to Smart Grid (e.g. SP800-131)

---

# CSWG Vulnerability Assessment Subgroup

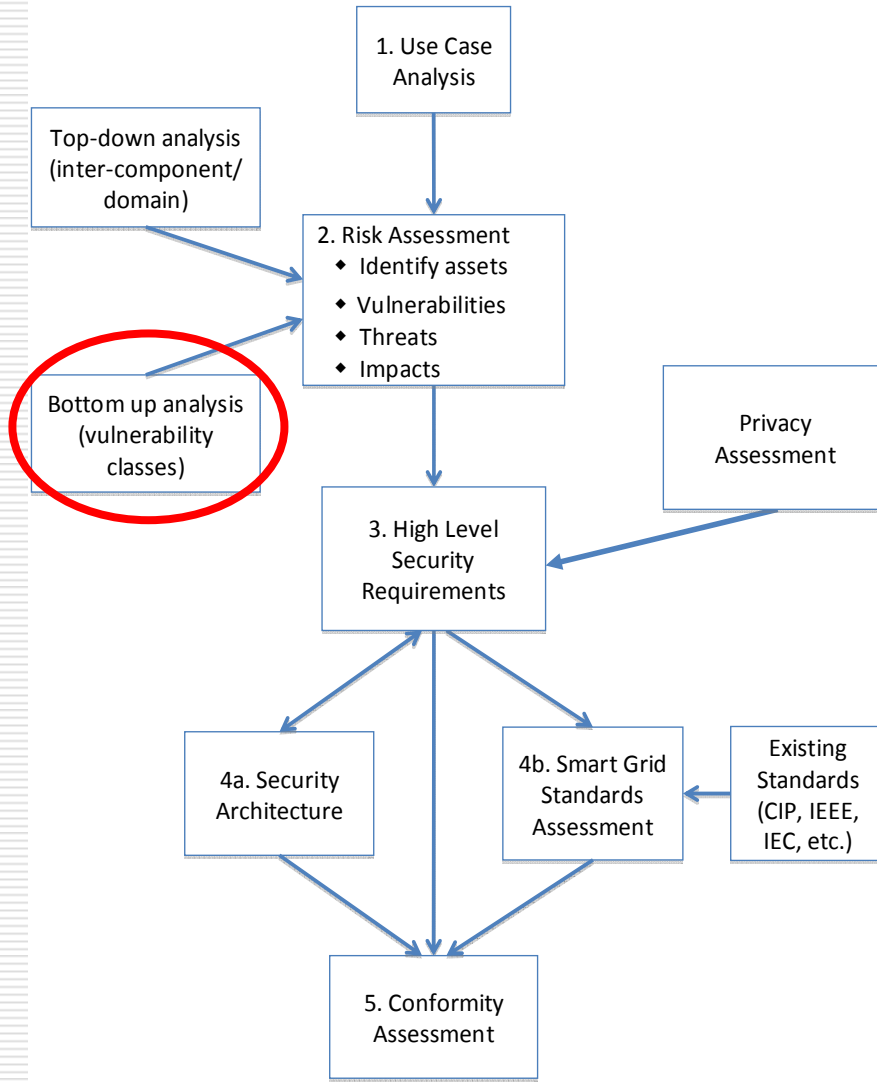
Leads:

Matt Carpenter ([matt@inguardians.com](mailto:matt@inguardians.com))

Matt Thomson ([matthew.thomson@ge.com](mailto:matthew.thomson@ge.com))

Twiki: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGVulnerabilities>

# Vulnerability Class Analysis



- Vulnerability classes
  - Category of weakness that could adversely impact the operation of the electric grid
- Intended Use by those responsible for designing, implementing, operating or procuring systems
- List of vulnerabilities that should be considered when making architectural and policy decisions
- This section is NOT a list of requirements
- No system contains none of these vulnerabilities

# Vulnerability Classes Chapter Content

---

- ❑ Not all possible vulnerabilities included
- ❑ Vulnerabilities classified by category
  - People, policy and procedure
    - ❑ Where a failure/deficiency in policies and procedures can lead to security risks for an organization
    - ❑ *Policies and procedures* are the documented mechanisms by which an organization operates
    - ❑ *People* are trained to follow them
  - Platform software/firmware vulnerabilities
    - ❑ Errors/oversight in software and firmware
      - Design
      - Development
      - Deployment
    - ❑ New instances continuously being discovered

# Vulnerability Classes Chapter Content (2)

---

- Platform Vulnerabilities
  - Platforms
    - Software and hardware units, systems of software/hardware, used to deliver software-based services
  - Vulnerabilities due to complexities of
    - Architecting
    - Configuring
    - Managing platform

# Example Vulnerability Class

---

- People, policy and procedure - personnel training associated with
  - Implementing
  - Maintaining
  - Operating Smart Grid information systems
  
- Example – inadequate security training and awareness program
  
- Programs should highlight the need for continuous retraining effort over organization-defined period of time
  - Continuously changing security profile
  - New procedures, new technologies, etc.

# Example Vulnerability Class (2)

---

## □ Examples

- Freely releasing information of someone's status
- Opening emails and attachments from unknown sources,
- Posting passwords for all to see

## □ Potential Impact

- Social engineering
  - One of the primary initiatives in acquiring as much information as possible
  - Giving one in some cases all the visibility, knowledge and opportunity to execute a successful attack

# Example Vulnerability Class (3)

---

- Platform software/firmware vulnerability – programmable components of a computing environment
  
- Example – password management vulnerability
  - Passwords are most commonly used form of authentication
  - Mistakes in handling passwords may allow an attacker to obtain/guess them

# Roadmap for Vulnerability Classes

---

- Design considerations
  - Expansion of material to cover more bottom-up problems and industry issues
  - Specification and solutions for standards and product development
- Specific topics
  - Authenticity and trust in supply chain
  - Vulnerability management and traceability in the supply chain
- Exploration of open and freely available standards

---

# CSWG Bottom-Up Analysis Subgroup

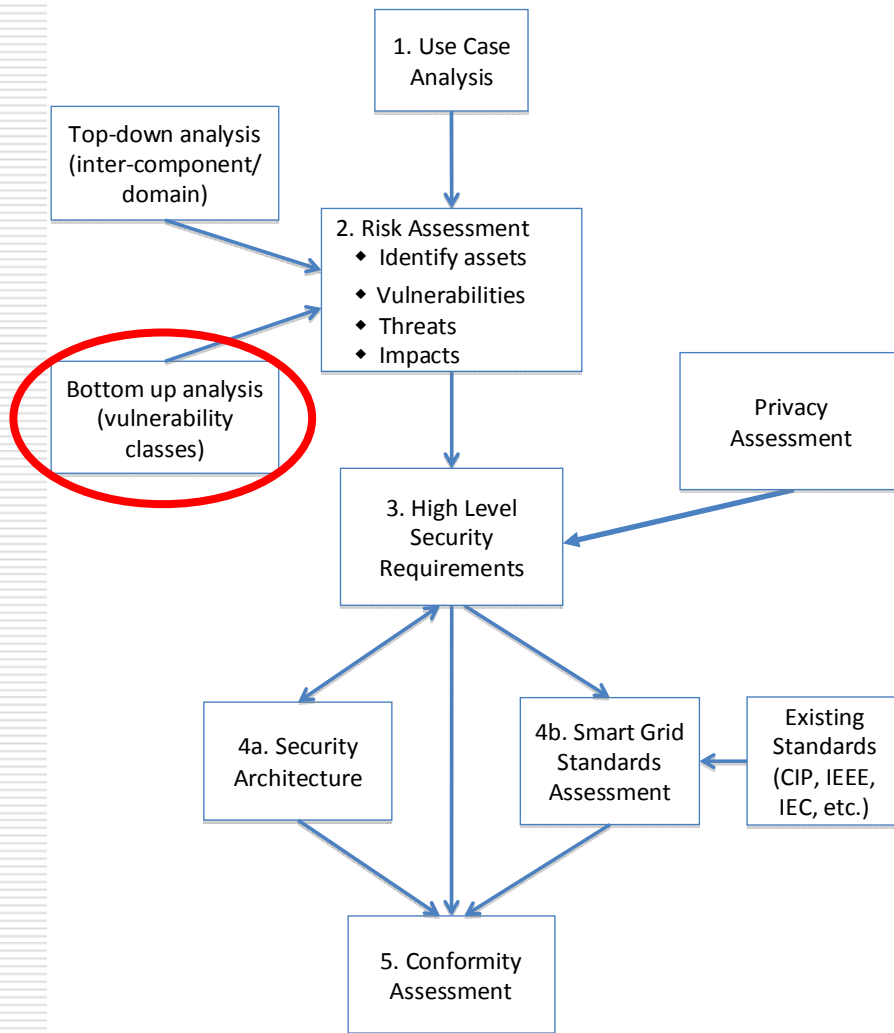
Leads:

Andrew Wight ([andrew.wright@n-dimension.com](mailto:andrew.wright@n-dimension.com))

Daniel Thanos ([daniel.thanos@ge.com](mailto:daniel.thanos@ge.com))

Twiki: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGBottomUp>

# Bottom-Up Analysis



- Identify: specific protocols, interfaces, applications, best practices, etc. that should be developed to solve specific Smart Grid cyber security problems
- Bottom-up approach
  - Identify some specific problems and issues that need to be addressed
  - Not to perform a comprehensive gap analysis that covers all issues.

# CSWG Bottom-Up Scope/Mission

---

- Intended to complement top-down work:
  - More quickly identify fruitful areas for solution development
  - Provide independent validation of top-down requirements
- Identify areas for solution development
- NOT a comprehensive gap analysis
- NOT specifying solutions
- NOT something that can be “complied with”

# Bottom-Up Chapter Content

---

- Evident and Specific Cyber Security Problems
  - 27 cyber security problems with specific relevance/uniqueness in Smart Grid
    - Authentication and Authorization
      - Users and Field Equipment
      - Maintenance personnel to meters
      - Consumers to meters, etc.
    - Insecure firmware updates
      - How to ensure malware is not installed
    - Absolute and accurate time information
      - Used by many types of power system devices for different functions
    - Openness and accessibility of Smart Grid standards
      - Barrier to evaluation and use of standards

# Bottom-Up Chapter Content (2)

---

- Non-Specific Cyber Security Issues
  - 33 cyber security issues that are too abstract to describe in terms of specific security problems
  - When considered in different contexts (control center, substation, meter, etc.) likely to lead to specific problems
  - Examples include
    - IT vs. Smart Grid
      - Differing scale, complexity and nature
    - Security model
      - Need different security levels that depend on network/system architecture design

# Bottom-Up Chapter Content (3)

---

- Design Considerations
  - 6 cyber security considerations that arise in design, deployment, and use of Smart Grid systems
  - Should be taken to account by system designers, implementers, purchasers, integrators, and users
  - NOT recommending specific solutions or requirements

# Sample Bottom-Up Cyber Security Issue

---

- Authenticating and Authorizing Consumers to Meters
  - Meters act as home area network gateways for providing energy information to consumers
  - Will consumers be authenticated to meters?
    - Authorization likely be highly limited
  - What would roles be?
    - Authorization and access levels need to be considered (i.e. consumer capable of supplying energy to power grid may have different access requirements)

# Sample Bottom-Up Non-Specific Cyber Security Issue

---

- IT vs. Smart Grid Security
  - Differences between IT, industrial and Smart Grid security need to be accentuated
  - NIST SP 800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*
    - Can be used as a basis
    - More needs to be addressed
    - Many differences in scale, complexity and environment of Smart Grid

---

# CSWG Research and Development (R&D) Subgroup

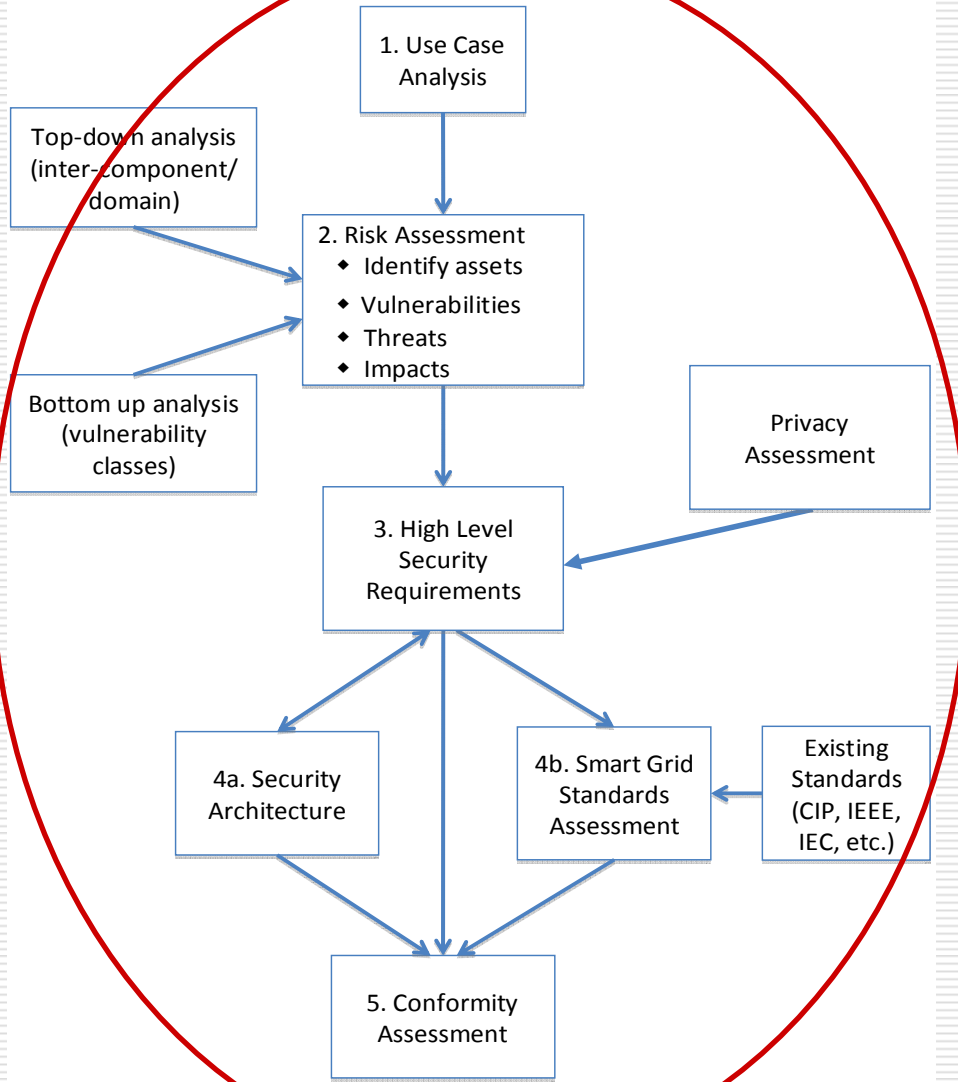
Leads:

Isaac Ghansah, California State University  
Sacramento ([ghansah@csus.edu](mailto:ghansah@csus.edu))

Daniel Thanos, GE Digital Energy  
([daniel.thanos@ge.com](mailto:daniel.thanos@ge.com))

Twiki: [http://collaborate.nist.gov/twiki-  
sggrid/bin/view/SmartGrid/CSCTGRandD](http://collaborate.nist.gov/twiki-<br/>sggrid/bin/view/SmartGrid/CSCTGRandD)

# Research and Development



- Research
  - Discovery of science supporting a product's viability (or lays the foundation for achieving a new target)
- Development
  - Turning something into a useful product or solution
  - *Engineering* refines a product/solution to make it economically viable.
- Discussion of problems that arise or are expected in Smart Grid that do not yet have commercially viable solutions
- Applies throughout Smart Grid Cyber Security Strategy

# R&D Subgroup Scope/Mission

---

- Identify R&D themes for cyber security in Smart Grid
  
- Focus on paradigm changing research to foster new/emerging security issues
  - Converged view of
    - IT
    - Communications
    - Power control systems
  
- Identify R&D needs and ideas as they are identified within the work of the CSWG

# R&D Chapter Content

---

- Written as an independent collection of research themes
  - Sections do not necessarily flow from introduction to summary
  
- Theme areas NOT categorized into
  - Long-term
  - Short-term
  - Research
  - Development
  
- High Level of R&D Themes to Smart Grid Cyber Security Requirements

# R&D Theme Areas

---

- Device Level
  - Cost-effective tamper-resistant architectures for resource-constrained devices (e.g. smart meters)
  
- Cryptography and Key Management
  - Need for
    - Large scale, economic key management
    - Cryptography on processors with strict space/computation limits
  - Security and privacy requirements for Smart Grid that may benefit from advanced cryptographic algorithms

# R&D Theme Areas (2)

---

## □ Systems Level

- Security and survivability architecture of Smart Grid
- Smart Grid must be
  - Built to adapt to changing needs in scale and functionality
  - Able to tolerate and survive malicious attacks of the present and future

## □ Networking Issues

- Economic and other drivers push use of commercial off-the shelf (COTS) components
  - Research needed to see if COTS can be used in Smart Grid reliably and safely
  - How they would be implemented

# R&D Theme Areas (3)

---

- Other Security Issues in the Smart Grid Context
  - Focus on models and other topics that do not fit cleanly into above areas
    - Infrastructure interdependency issues
      - Resiliency and continuous availability of power grid critical to national infrastructure
    - Denial of service resiliency
      - More opportunities for exploitation of IP-based transport protocols

# Example R&D Topic

---

- Legacy system integration
  
- Challenges
  - Compatibility problems
    - New security solutions are installed in new devices
    - Mismatched expectations that may cause the devices to fail or malfunction
    - Backwards compatibility
      - May prevent deployment of advanced features
  - Potential avenues of investigation
    - Compositionality (enhanced overlays, bump in wire, adapters) that contain and mask legacy systems and
    - Ensuring that the weakest link does not negate new architectures
      - Formal analysis and validation of the architectural design, possibly using red team methodology

# Next Steps

---

- Future Topics Pending Official Mandate from NIST
  - Synchrophasor Security/ NASPInet
  - Anonymization
  - Use of IPv6 in large scale real time control systems
  - Behavioral Economics/Privacy
  - Cross-Domain security involving IT, Power, and Transportation systems
  - Remote Disablement/Switch of Energy Sources
  
- Refinement of Mapping to Smart Grid Cyber Security Requirements

---

# CSWG Standards Assessment Subgroup

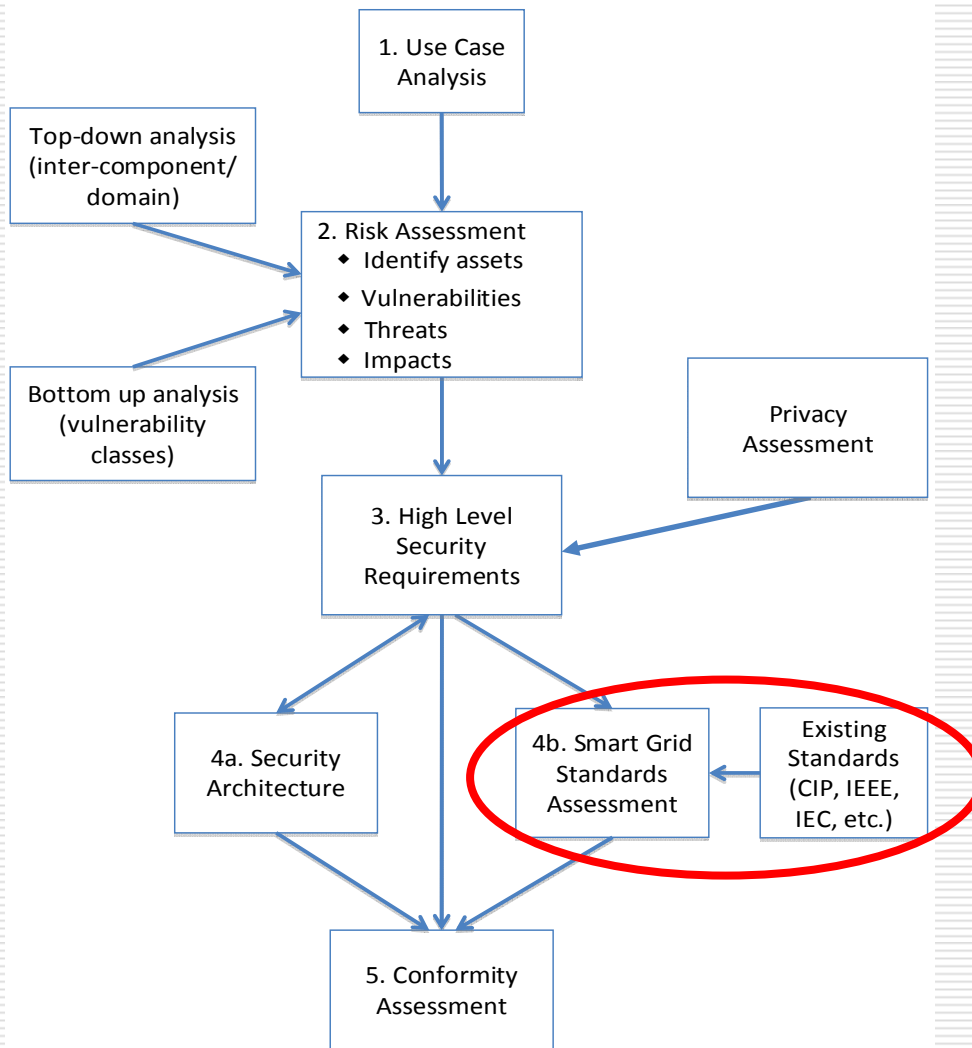
Leads:

Virginia Lee ([vlee@ecompcounselants.com](mailto:vlee@ecompcounselants.com))

Frances Cleveland ([fcleve@xanthus-consulting.com](mailto:fcleve@xanthus-consulting.com))

Twiki: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGStandards>

# CSWG Standards Subgroup



□ Identify and assess the cyber security related standards that are used in smart grid applications to ensure adequate cyber security coverage is included

□ Where adequate coverage is not included

■ Recommend changes that should be made to the standard or other standards that should be applied

# Standards Assessment

---

- Assessment of Standards
  - Identified initial set of standards submitted for review and assessment in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0
  - Assessment of the initial list of standards is underway
  - Results will appear in a separate document titled: *Summary of Use, Application, Cyber Security, and Functionality of Smart Grid Interoperability Standards Identified by NIST (Standards Assessment)*

# Standards Assessment (2)

---

- The NISTIR Standards Section
  - The review process is outlined in the Standards section of the NISTIR
  - Each standard will be reviewed by multiple reviewers
    - Manufacturing/Suppliers
    - IT/Telecom
    - Utility Sector
  - Assessment template is included with a description of the content the assessment should produce
  - List of standards being assessed and their assessments NOT included in this document

# Standards Assessment (3)

---

- Will include mapping to the security requirement families identified in the High Level Requirements chapter
  
- For Cryptography requirements, the assessment will address:
  - Algorithm
  - Mode
  - Key Size
  
- For other referenced standards
  - Required that the referenced standard be included in this phase of the review

# Standards Assessment Sample Questions

---

- ❑ Standard number and version
- ❑ Standard Name
- ❑ Does the standard cover cyber security?
  - Describe any gap(s) in coverage:
- ❑ Repeat this per standard section
  - Standard section/chapter/page reference
  - Applicable NISTIR security family
  - Applicable NISTIR requirement
  - Does the standard meet the security requirement?
- ❑ Is crypto included in the standard?
  - Does the standard meet the crypto requirements?
- ❑ List any referenced standards

# Standards Assessment Next Steps

---

- Current assessment process
  - Individual team member reviews of assessments
  - Collaboration sessions for reaching agreement on final assessments to submit for management review
  
- Perform NIST management team review
  
- Submit standards for inclusion in *NIST Standards Assessment* document

# Standards Assessment Next Steps (2)

---

- Standards Team Disposition
  - Process identified will continue for the next list of standards provided to the team
  - Team will be ongoing
    - Continue to provide assessments
    - Provide updates to the *NIST Standards Assessment Document*

# Wrap-up

---

- Thank you to everyone for joining us today
  
- If interested in future involvement with the CSWG, our weekly teleconference information is as follows:
  - Mondays, 11:00 AM Eastern
  - Call in number: 866-745-6097
  - Participant passcode: 7413006
  
  - Twiki: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG>