



Managing SCADA Security

NISTIR 7628 and the NIST/SGIP CSWG

May 25, 2011

Frances Cleveland

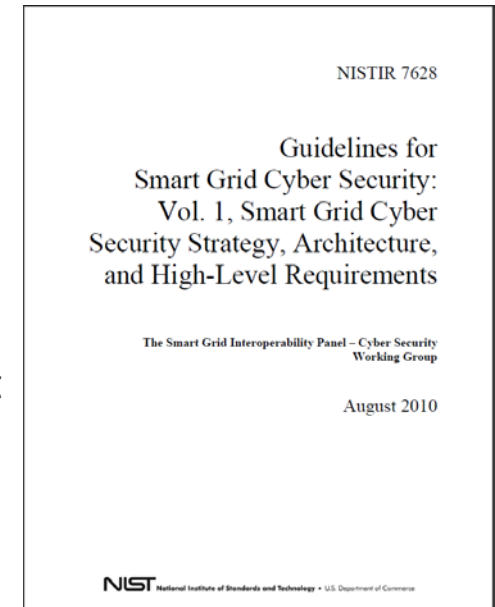
fcleve@xanthus-consulting.com

Topics

- NISTIR 7628
- NIST/SGIP CSWG and its Subgroups
- CSWG Standards Subgroup
- DOE-funded NESCO / NESCOR

NIST Cyber Security Activities

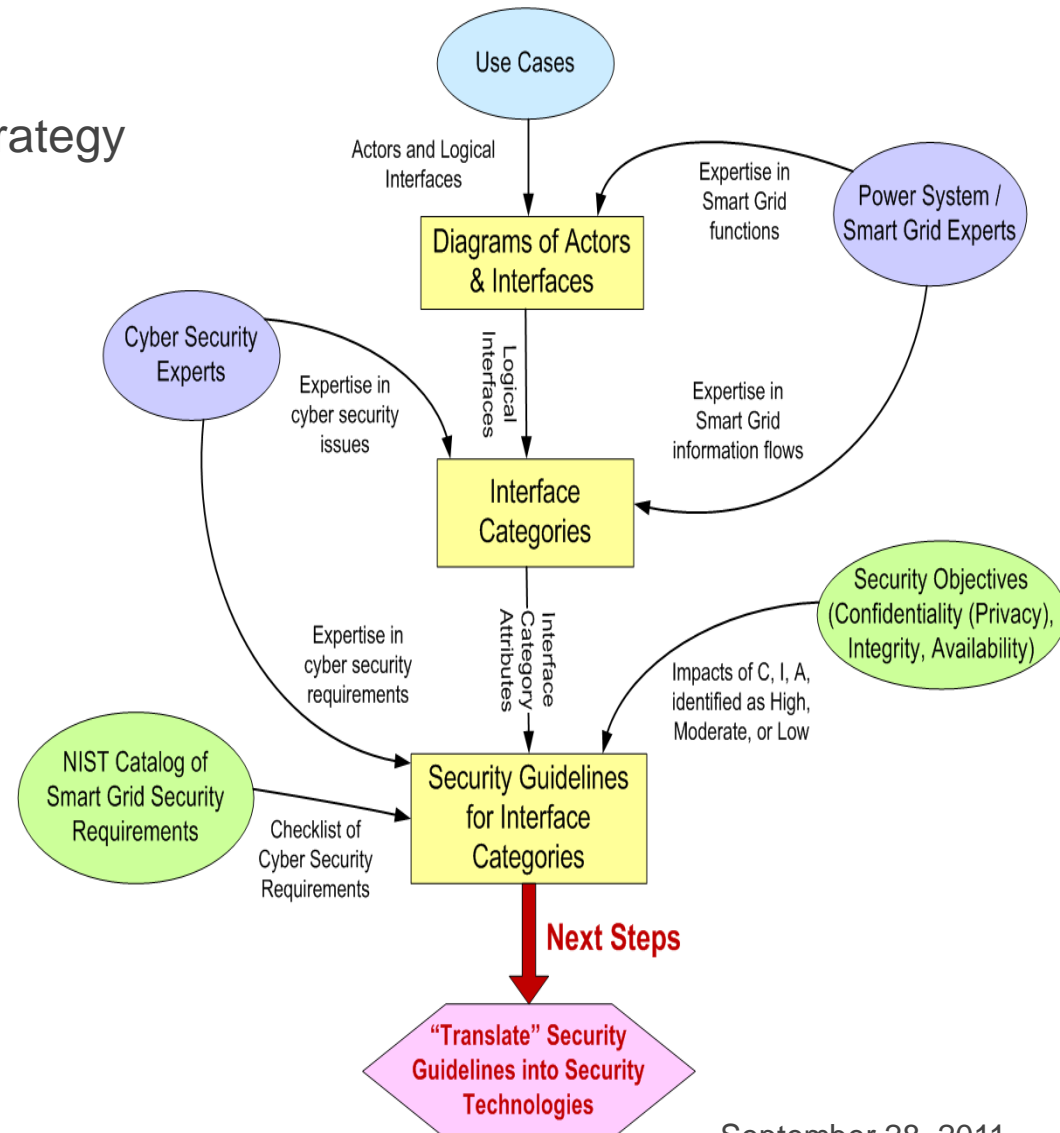
- NIST established the Cyber Security Working Group (CSWG) in 2009
 - Has over 500 members
 - Has established many (>12) very active Subgroups, including High Level Requirements, Vulnerabilities, Bottom-Up, Architecture, Standards Assessment, Design Principles, and Privacy
 - Established liaisons with NERC, and influenced their next CIP versions
- CSWG Goal:
 - Develop an overall cyber security strategy for the Smart Grid that includes a risk mitigation strategy to ensure interoperability
 - Include prevention, detection, response, and recovery
- Developed the NIST Interagency Report (NISTIR) 7628
 - Published in August 2010
 - Updates every 18 months



NISTIR 7628: Guidelines for Smart Grid Cyber Security

NIST Cyber Security Guidelines: Development Process

- Volume 1:
 - Smart Grid Cyber Security Strategy
 - Architecture
 - High Level Requirements
 - Key Management
- Volume 2:
 - Privacy
- Volume 3:
 - Vulnerabilities
 - “Bottom-Up” Issues
 - Research and Development
 - Other supportive material



NIST Cyber Security Strategy

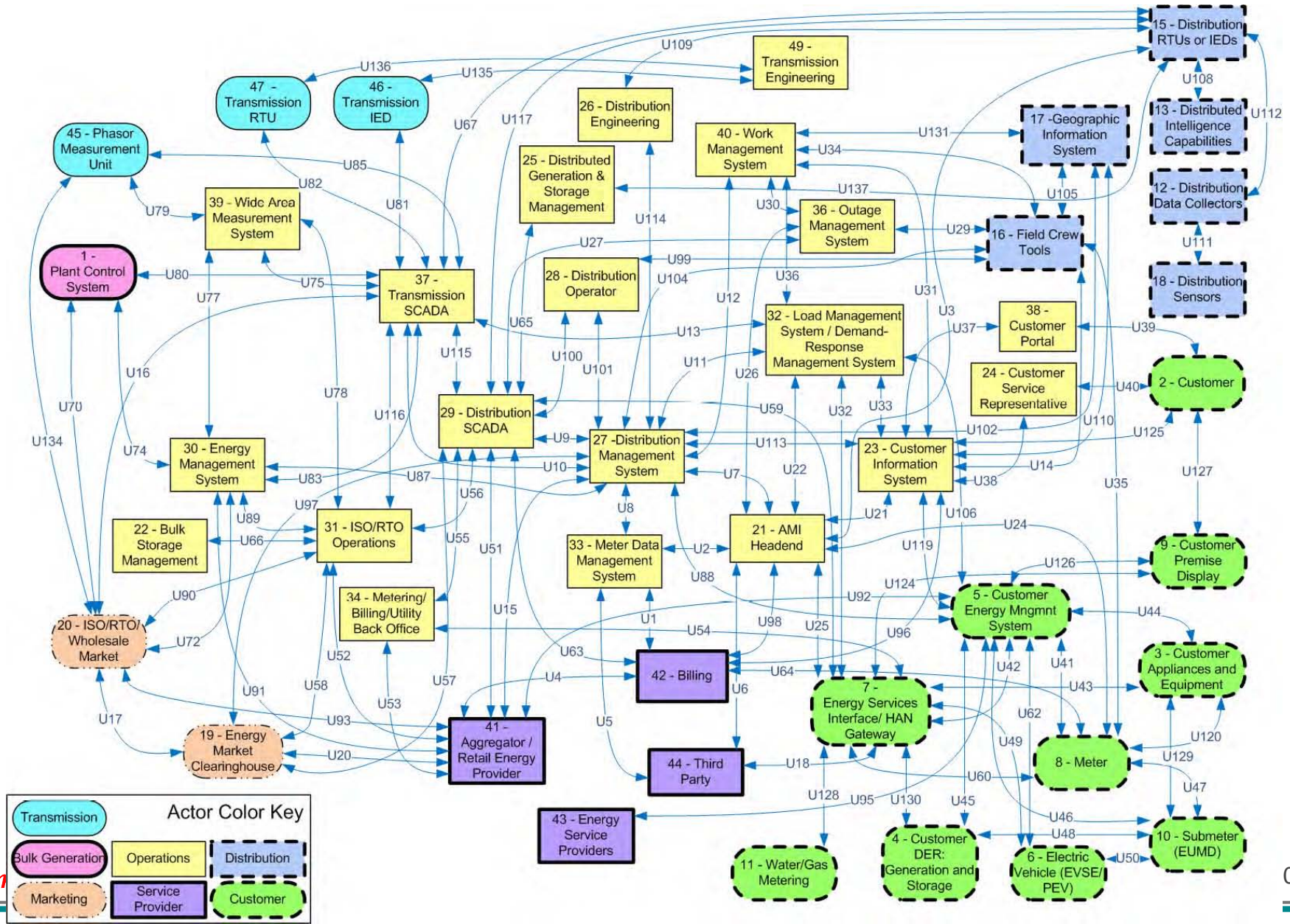
- **All-Hazards Approach**
 - Deliberate cyber attacks
 - Inadvertent compromises / mistakes / equipment failures
 - Natural disasters
- Recognition of Key Requirement: **Power System Reliability**
 - Use of “IT” security measures: Risk assessment, role-based access, key management
 - Use of existing power system engineering and applications for reliability
 - Extend and upgrade engineering and applications
- Newer Areas: **Confidentiality and Privacy**
 - Privacy for customer-related personal information – particularly related to Smart Meters
 - Confidentiality for market, financial, corporate, and other sensitive information
- **Defense in depth**: policy, prevention, detection, notification, coping, recovery, auditing

NIST High Level Cybersecurity Requirements

- Security Architecture based on “FERC 4 + 2” diagrams that identified key interfaces
- Security Requirements Analysis is based on a number of components:
 - **Diagrams of logical interfaces** between actors in the Smart Grid
 - **Interface Categories** that allow the hundreds of logical interfaces to be organized and categorized
 - **Smart Grid Catalog of Security Requirements** applied to Interface Categories
 - Excellent checklist for security requirements!

NIST Architecture Diagram (Spaghetti Diagram)

(an example of why the NISTIR needs “interpretation”)



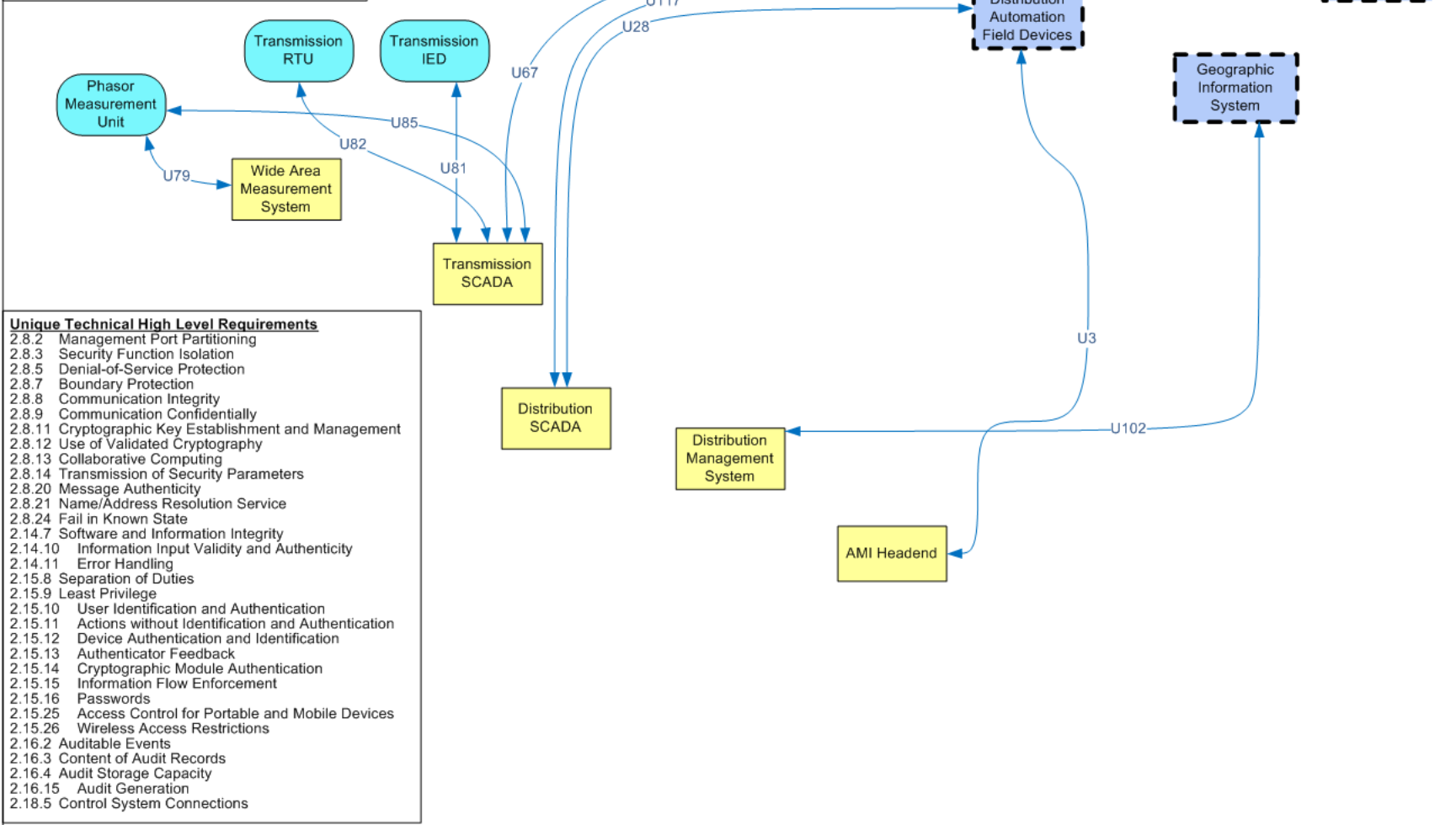
NIST Security Interface Categories

- Over 100 Logical Interfaces between Actors
 - Logical interfaces are drawn between actors in the diagrams
 - Need to organize and categorize the hundreds of logical interfaces
- Attributes of these logical interfaces were used to develop 22 Interface Categories. Examples include:
 - 1 – 4 cover communications between control systems and field equipment with different availability and media constraints
 - 5 – 6 cover the interfaces between control systems either within the same organization or between organizations
 - 10 covers the interfaces between control systems and non-control/corporate systems
 - 14 covers the interfaces between systems that use the AMI network with high availability requirements, such as for Distribution Automation

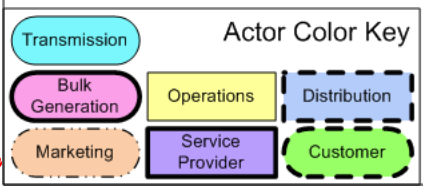
Confidentiality: **LOW**
 Integrity: **HIGH**
 Availability: **HIGH**

Interface Category 1

Interface Category 1a Definition:
 Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example:
 - Between transmission SCADA and substation equipment
 - Between distribution SCADA and high priority substation and pole-top equipment
 - Between SCADA and DCS within a power plant



- Unique Technical High Level Requirements**
- 2.8.2 Management Port Partitioning
 - 2.8.3 Security Function Isolation
 - 2.8.5 Denial-of-Service Protection
 - 2.8.7 Boundary Protection
 - 2.8.8 Communication Integrity
 - 2.8.9 Communication Confidentiality
 - 2.8.11 Cryptographic Key Establishment and Management
 - 2.8.12 Use of Validated Cryptography
 - 2.8.13 Collaborative Computing
 - 2.8.14 Transmission of Security Parameters
 - 2.8.20 Message Authenticity
 - 2.8.21 Name/Address Resolution Service
 - 2.8.24 Fail in Known State
 - 2.14.7 Software and Information Integrity
 - 2.14.10 Information Input Validity and Authenticity
 - 2.14.11 Error Handling
 - 2.15.8 Separation of Duties
 - 2.15.9 Least Privilege
 - 2.15.10 User Identification and Authentication
 - 2.15.11 Actions without Identification and Authentication
 - 2.15.12 Device Authentication and Identification
 - 2.15.13 Authenticator Feedback
 - 2.15.14 Cryptographic Module Authentication
 - 2.15.15 Information Flow Enforcement
 - 2.15.16 Passwords
 - 2.15.25 Access Control for Portable and Mobile Devices
 - 2.15.26 Wireless Access Restrictions
 - 2.16.2 Auditable Events
 - 2.16.3 Content of Audit Records
 - 2.16.4 Audit Storage Capacity
 - 2.16.15 Audit Generation
 - 2.18.5 Control System Connections



NIST Catalog of Smart Grid Cyber Security Requirements – Excellent Checklist!

Ref.	NIST Smart Grid Security Requirements Families
SG.AC	Access Control
SG.AT	Security Awareness and Training
SG.AU	Audit and Accountability
SG.CA	Security Assessment and Authorization
SG.CM	Configuration Management
SG.CP	Continuity of Operations
SG.IA	Identification and Authentication
SG.ID	Information and Document Management
SG.IR	Incident Response
SG.MA	Smart Grid system Development and Maintenance
SG.MP	Media Protection
SG.PE	Physical and Environmental Security
SG.PL	Strategic Planning
SG.PM	Security Program Management
SG.PS	Personnel Security
SG.RA	Risk Management and Assessment
SG.SA	Smart Grid System and Services Acquisition
SG.SC	Smart Grid System and Communication Protection
SG.SI	Smart Grid System and Information Integrity

CSWG Standards Subgroup

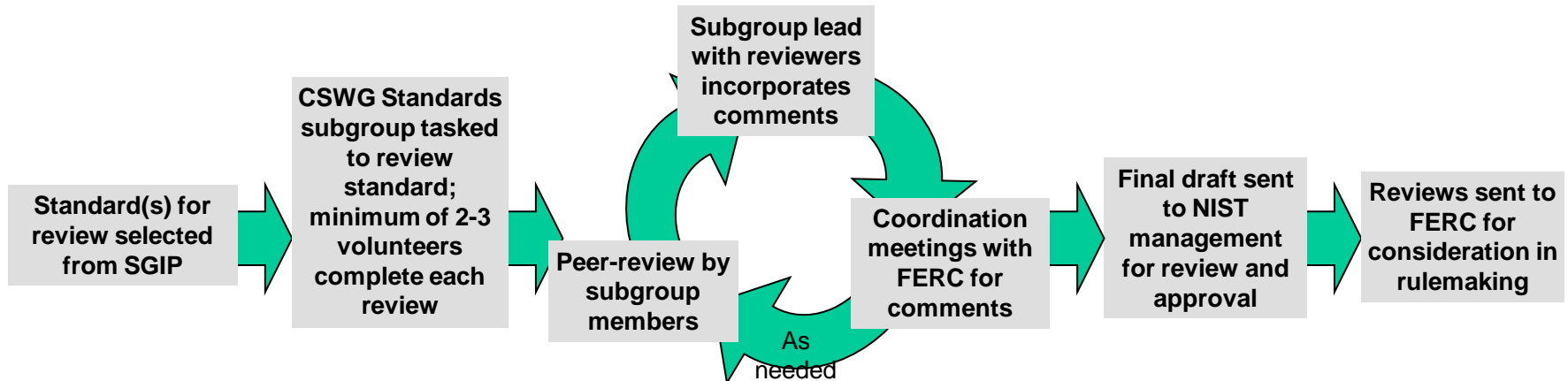
- Mission
 - Identify and assess the cyber security contained within standards and other documents that are commonly used in smart grid applications to ensure adequate cyber security coverage is included
 - Where adequate coverage is not included, to recommend changes that should be made to the standard or other standards that should be applied
- Assessment process of a standard or document:
 - Develop a small team of CSWG Standards members, enhanced with experts familiar with document
 - Use CSWG template (Word document) for consistency
 - Describe document briefly, focusing on cybersecurity aspects
 - Correlate existing cybersecurity requirements with the NISTIR catalog of cybersecurity requirements
 - Identify cybersecurity gaps or problems
 - Recommend actions and changes within the document if possible or with a new document
- <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSC TGStandards>

CSWG Standards Assessment Process

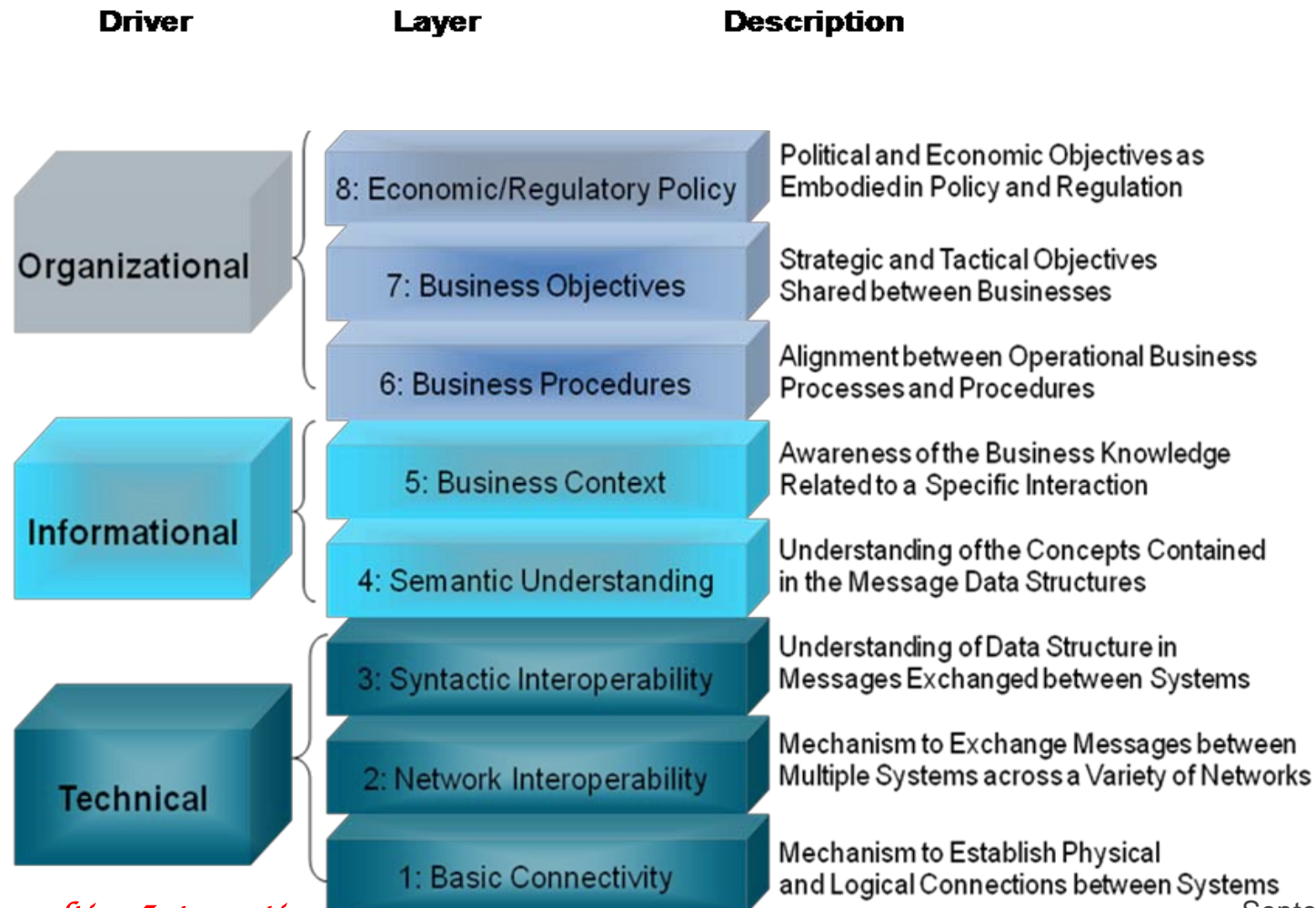
For Priority Action Plan (PAP) Documents:



For Documents Listed in the NIST Framework Document, NIST SP 1108 :



Standards Must Be Assessed at their Appropriate GWAC Stack Layer



Standards and Documents Reviewed by the CSWG Standards Subgroup

- IEC Standards: IEC 60870-6 (ICCP), IEC 61850, IEC 61968/70 (CIM), IEC 62351 (Security)
- PAP 0: NEMA SG-AMI 1-2009: Requirements for Smart Meter Upgradeability
- PAP 1: Internet Protocol Suite
- PAP 2: Wireless Standards for the Smart Grid
- PAP 4: OASIS WS-Calendar
- PAP 5: AEIC Guidelines for ANSI C12.19
- PAP 10: NAESB Energy Usage Information
- PAP 11: SAE J1772-3, SAE J2836-1, SAE J2847-1
- PAP 13: IEEE 1588:2008, IEC 61850-90-5, IEEE PC37.238™/D5.7
- ANSI C12.1, ANSI C12.18, ANSI C12.19, ANSI C12.21, ANSI C12.22
- Zigbee Alliance SEP 2.0 TRD, 095449 Version 0.7, SEP 2.0 Application Protocol Specification, 11167 Version 0.7
- Zigbee Alliance (in progress): SEP 1.0, SEP 1.1
- PAP 12 (in progress): IEEE 1815 (DNP3), IEEE 1815.1 (Mapping between DNP3 and IEC 61850)
- PAP 15 (in progress): IEEE 1901™-2010, ITU-T G.9972

DOE-funded National Electric Sector Cybersecurity Organization (NESCO)

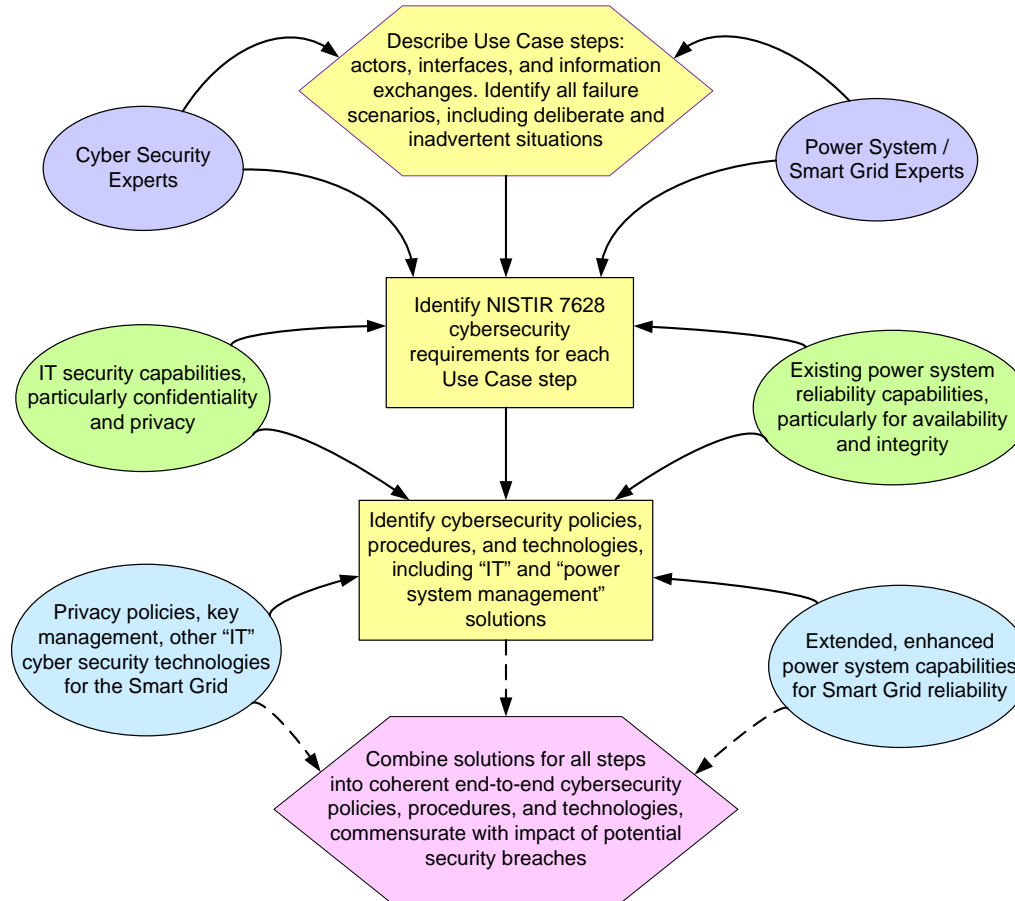
- **National Electric Sector Cybersecurity Organization (NESCO)** is the first public-private partnership of its kind in the electric sector, initiated in Q1 of 2011.
 - NESCO serves as a focal point bringing together utilities, federal agencies, regulators, researchers, academics, and international experts.
 - Identify and disseminate common, effective cyber security practices
 - Analyze, monitor and relay infrastructure threat information
 - Focus cyber security research and development priorities
 - Work with federal agencies to improve electric sector cyber security
 - Encourage key electric sector supplier and vendor support / interaction
 - EnergySec coordinates this project
 - EPRI provides technical resources (NESCOR)
 - Working closely with the CSWG to provide mutual benefits

Next Steps: How to Apply the NISTIR to Smart Grid Use Cases

- Involve both Cybersecurity experts and Power System/Smart Grid experts from the beginning
- Describe Use Case steps and identify all failure scenarios, including deliberate and inadvertent situations
 - Power system experts describe the actors, interfaces, and the types of information to be exchanged. They also cover existing power system reliability capabilities, particularly for availability and integrity
 - IT cybersecurity experts address security failure scenarios and vulnerabilities, particularly confidentiality and privacy
- Identify NISTIR 7628 cybersecurity requirements for each Use Case step
- Identify cybersecurity policies, procedures, and technologies, including “IT” and “Power system management” solutions
 - Power system experts focus on extended, enhanced power system capabilities that could improve Smart Grid reliability
 - IT cybersecurity experts focus on privacy policies, key management, and other “IT” cyber security technologies for the Smart Grid
- Combine solutions for all Use Case steps into coherent end-to-end cybersecurity policies, procedures, and technologies, commensurate with the impact of potential security breaches
 - More than one combination of potential solutions would be expected
 - The results should be balanced approaches, with the cost of cybersecurity solutions commensurate with the cost of the impact of a security breach times the likelihood of such a breach.

Next Steps: How to Apply the NISTIR to Smart Grid Use Cases

How to Apply NISTIR 7628 Cybersecurity Requirements to Smart Grid Use Cases





Questions?

Frances Cleveland

fcleve@xanthus-consulting.com