



NIST Cyber Security Working Group (CSWG)

NISTIR 7628: NIST Guidelines for Smart Grid Cyber Security

Frances Cleveland

Xanthus Consulting International

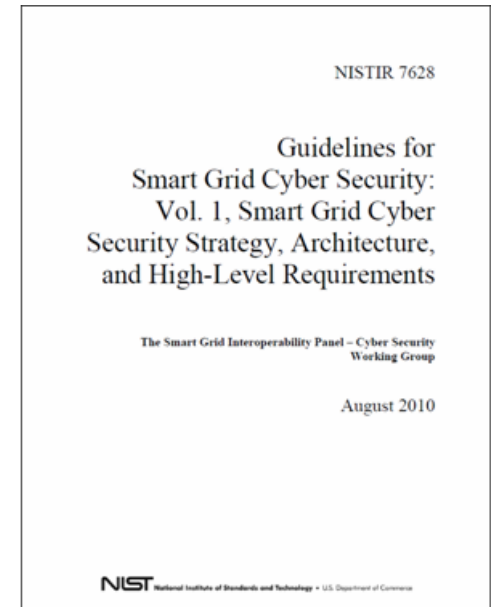
fcleve@xanthus-consulting.com

Topics

- NIST Cyber Security Activities
- NISTIR 7626 Guidelines for Smart Grid Cyber Security
- CSWG Standards Subgroup: Assessment of Information Exchange Standards
- CSWG Privacy Subgroup: Addressing privacy issues for the Smart Grid

NIST Cyber Security Activities

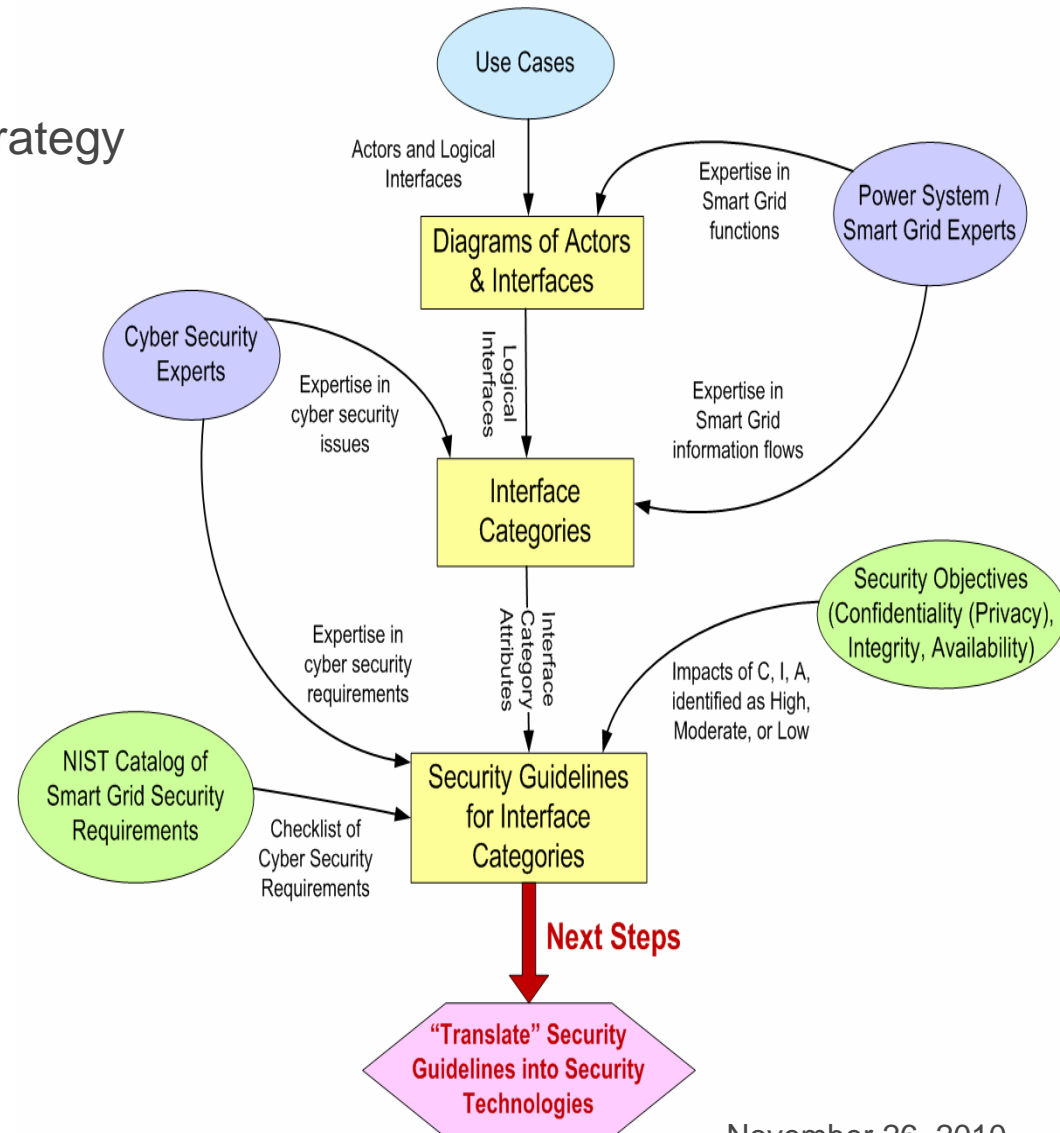
- NIST established the Cyber Security Working Group (CSWG) in 2009
 - Originally called the CSCTG
 - Has over 500 members
 - Has established many (>12) very active Subgroups, including High Level Requirements, Vulnerabilities, Bottom-Up, Architecture, Standards Assessment, and Privacy
 - Established 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



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 attacks
 - Inadvertent compromises
 - Natural disasters
- Recognition of Key Requirement: Power System Reliability
 - Use of “IT” security measures: role-based access, key management
 - Use of existing power system engineering and applications for reliability
 - Extend and upgrade engineering and applications
- Newer Area: 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 Security 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 Security Interface Categories

- Interface categories are used to organize and categorize the hundreds of logical interfaces
 - Logical interfaces are drawn between actors in the diagrams
- Attributes of these logical interfaces were used to develop 22 Categories. Examples include:
 - 1 – 4 cover communications between control systems (typically centralized applications such as a SCADA master station) and equipment as well as communications between 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

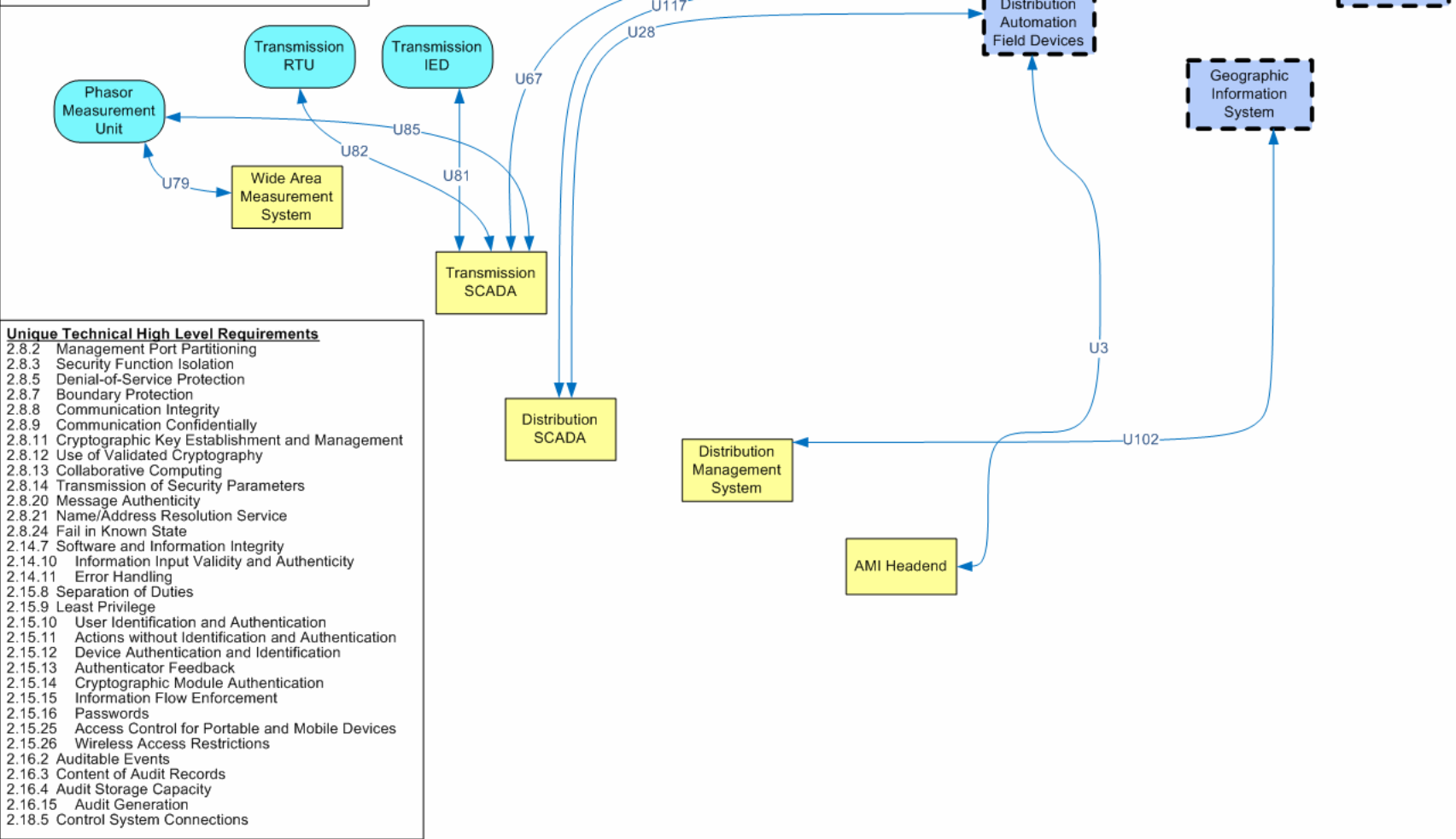
Interface Category 1a Definition:

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

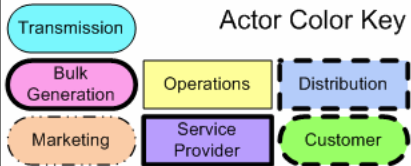
Confidentiality: **LOW**
Integrity: **HIGH**
Availability: **HIGH**

Interface Category 1



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



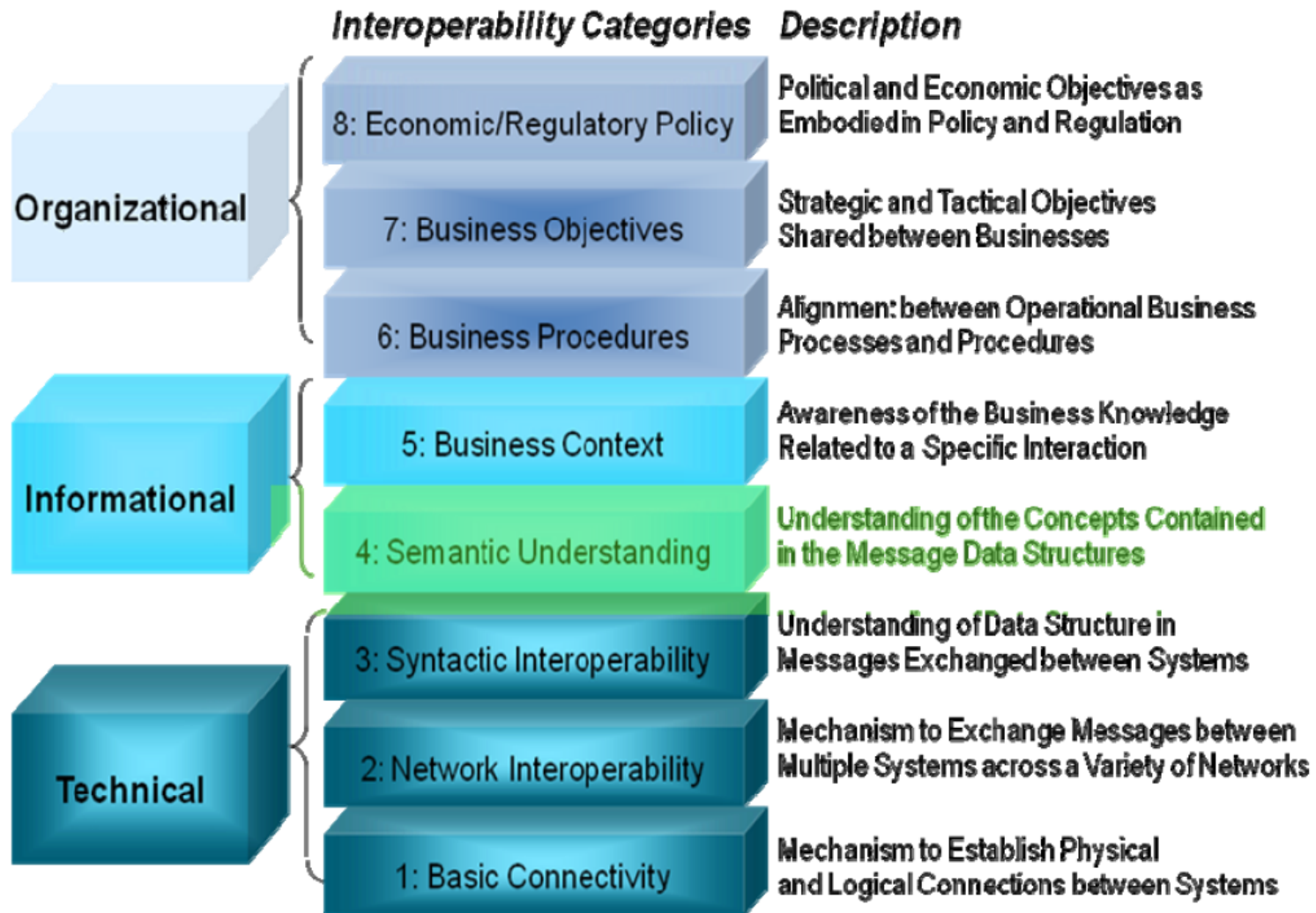
NIST Catalog of Smart Grid Cyber Security Requirements – Excellent Checklist!

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 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
- Have assessed 5 IEC standards and submitted them to FERC
- Have just finished assessing 9 standards from the NIST Priority Action Plans (PAPs)
- <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGStandards>

Important Note: Assess Standards at their Appropriate GWAC Stack Layer



Five IEC Interoperability Standards Reviewed by NIST for Cyber Security Gaps, then Passed to FERC

- IEC 60870-6 (better known as IEC 60870-6-2) (better known as ICCP)
 - Security provided by IEC 62351-3 (TLS over TCP/IP) and -4 (for MMS)
- IEC 61970 (Common Information Model (CIM) for transmission wires modeling)
 - Abstract “Semantic Model” so no security needed in the standard
- IEC 61968 (CIM for distribution, AMI interfaces, asset management)
 - Abstract “Semantic Model” so no security needed in the standard
 - Recognition that security for CIM implementations is still lacking
- IEC 61850 (for substation automation, distribution automation, and Distributed Energy Resources (DER))
 - Security provided by IEC 62351-3 (TLS over TCP/IP), -4 (for MMS), and -6 (for GOOSE)
- IEC 62351 Cyber Security Series (1-8)

One Security Standard Assessment: IEC 62351

Mapping of TC57 Communication Standards to IEC 62351 Security Standards

IEC 62351 Part 1: Introduction

IEC 62351 Part 2: Glossary

IEC 60870-6 TASE.2

IEC 62351 Part 3: Profiles Including TCP/IP

IEC 61850 over MMS

IEC 62351 Part 4: Profiles Including MMS

IEC 61850 GOOSE, GSE, SMV

IEC 62351 Part 5: IEC 60870-5 & Derivatives

IEC 60870-5-104 & DNP3

IEC 62351 Part 6: IEC 61850

IEC 60870-5-101 & Serial DNP

IEC 62351 Part 8: Role-Based Access Control (RBAC)

IEC 62351 Part 7: Objets for Network Management

Nine “Standards” Released by NIST Priority Action Plans (PAPs)

- PAP 0: Meter Upgradeability Guidelines – addressed cyber security appropriately and mostly completely
- PAP 1: Internet Protocol Suite – IPsec and TLS. Recommended improved network and system management by “combining” SNMP and NetConf
- PAP 2: Wireless – identified cyber security measures at individual equipment level, but not at wireless system level
- PAP 4: Scheduling – ws-calendar is an abstract model, so no need to address cyber security in the standard
- PAP 5: Metering – identified some security issues with ANSI C12.xx

Nine “Standards” Released by NIST Priority Action Plans (PAPs)

- PAP 10: Energy Usage – the NAESB Energy Usage models are abstract, so no need to address cyber security in the standard
- PAP 11: Plug-In Electric Vehicles – 3 standards
 - Two SAE standards were acceptable from a cyber security perspective with some recommendations (electrical charger connections and PEV Use Cases)
 - Mapping of CIM PEV messages to SEP 2.0 has serious cyber security and design problems (partially since SEP 2.0 does not exist yet)

Next Standards Assessment Efforts

- Next standards to be assessed will be the “AMI” Standards, including the ANSI C12.xx series
- In the works ---
 - PAP 7: Energy Storage and Distributed Energy Resources (ES-DER) – defined in IEC 61850-7-420 and being mapped to both SEP 2.0 and DNP3
 - PAP 8: Distribution Management – Use Cases being defined in IEC 61850 (interactions with field devices) and in CIM (application-to-application interactions)
 - PAP 12: Mapping between IEC 61850 and DNP3 (being used in PAP 7)

CSWG Privacy Subgroup

- NISTIR 7628 contains a very general discussion of privacy issues and concerns
- Clarifies the distinction between Confidentiality (business, market, safety concerns) and Privacy (personal information).
- Regulators will ultimately be responsible for stating privacy requirements.
 - Need support to understand the privacy implications of certain types of energy-related information
 - CSWG has on-going work to try to understand what types of data should be private, and to what degree/level (e.g. aggregated data is less private than individual data)
 - Including new areas of PEVs, distributed generation, customer reactions to demand response requests, etc.
- Privacy team consists primarily of privacy experts
 - Need utility expertise, particularly those involved in AMI, demand response, DER management, and customer interactions
 - Need better understanding of what types of privacy policies may be mandated or need to be addressed by regulators and policy makers



Questions?

Frances Cleveland

fcleve@xanthus-consulting.com



Xanthus

Consulting International