DRAFT NISTIR 7628

Smart Grid Cyber Security Strategy and Requirements

The Smart Grid Interoperability Panel – Cyber Security Working Group

February 2010

NIST National Institute of Standards and Technology • U.S. Department of Commerce

DRAFT NISTIR 7628

Smart Grid Cyber Security Strategy and Requirements

The Smart Grid Interoperability Panel–Cyber Security Working Group

February 2010

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7628 (draft)
305 pages (February 2010)

Acknowledgments

This document was developed by members of the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG), formerly the Cyber Security Coordination Task Group (CSCTG). The group is chaired by Annabelle Lee of NIST. Tanya Brewer of NIST is the editor of this document. The members of the SGIP-CSWG have extensive technical expertise, knowledge, and commitment to addressing the cyber security needs of the Smart Grid. Members of the SGIP-CSWG and the working groups of the SGIP-CSWG are listed in Appendix G of this document.

Another group has also been instrumental in the development of a previous version of this document. The Advanced Security Acceleration Project – Smart Grid (ASAP-SG) developed the security profile for Advanced Metering Infrastructure (AMI) for the SGIP - CSWG and The UtiliSec Working Group (UCAIug). Many of the members of the ASAP-SG also participate in the SGIP-CSWG.

Table of Contents

EXECUTIVE SUMMARY

Smart Grid technologies will introduce millions of new intelligent components to the electric grid that communicate in a much more advanced ways (two-way, with open protocols) than in the past. Because of this, two areas that are critically important to get correct are Cyber Security and Privacy. The Cyber Security Strategy and Requirements began with the establishment of a Cyber Security Coordination Task Group (CSCTG) led by the National Institute of Standards and Technology (NIST) that now contains more than 350 participants from the private sector (including vendors and service providers), academia, regulatory organizations, and federal agencies. This group has been renamed under the Smart Grid Interoperability Panel (SGIP) to Cyber Security Working Group (SGIP–CSWG). Cyber security is being addressed using a thorough process that will result in a comprehensive set of cyber security requirements. As explained more fully in the first chapter, these requirements are being developed using a high-level risk assessment process that is defined in the cyber security strategy for the Smart Grid. Cyber security requirements are implicitly recognized as critical in all of the priority action plans discussed in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST Special Publication 1108)1 document that was published in January 2010.

CYBER SECURITY STRATEGY FOR THE SMART GRID

The overall cyber security strategy for the Smart Grid examines both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The primary goal of the cyber security strategy should be on prevention. However, it also requires that a response and recovery strategy be developed in the event of a cyber attack on the electric system.

Implementation of a cyber security strategy requires the definition and implementation of an overall cyber security risk assessment process for the Smart Grid. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. This type of risk is one component of organizational risk. Organizational risk can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk, and the risk from information systems). The Smart Grid risk assessment process is based on existing risk assessment approaches developed by both the private and public sectors and includes identifying impact, vulnerability, and threat information to produce an assessment of risk to the Smart Grid and to its domains and sub-domains, such as homes and businesses. Because the Smart Grid includes systems from the IT, telecommunications, and energy sectors, the risk assessment process is applied to all three sectors as they interact in the Smart Grid.

Following the risk assessment, the next step in the Smart Grid cyber security strategy is to select and tailor (as necessary) the security requirements. The documents used in this step are listed under Task 3 below.

The security requirements and the supporting analysis that are included in this NIST report may be used by implementers of the Smart Grid, e.g., utilities, equipment manufacturers, regulators,

[1] Available at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf

as input to their risk assessment processes. The information serves as baseline guidance to the various organizations for assessing risk and selecting appropriate security requirements. In addition, each organization should develop its own cyber security strategy for the Smart Grid.

Figure 1.1 illustrates the tasks defined for the Smart Grid cyber security strategy. The tasks are defined after the figure.

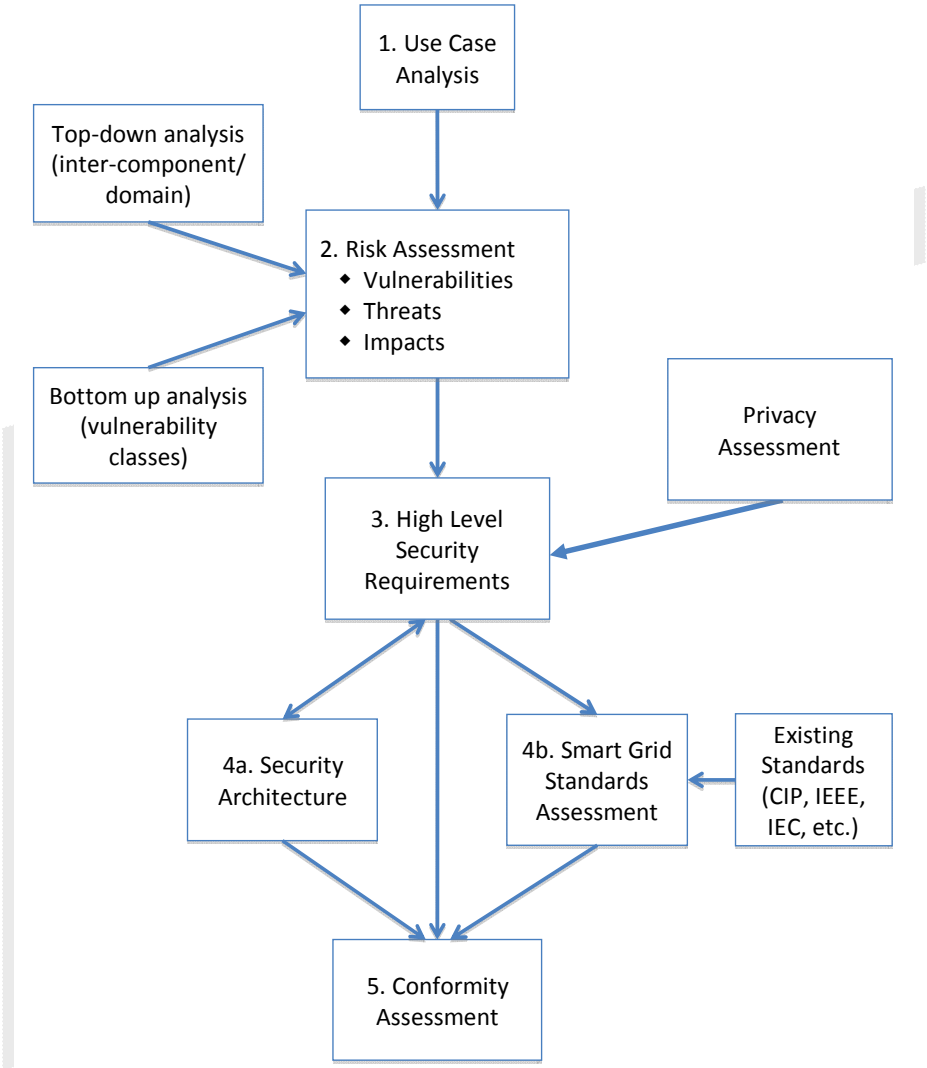

Figure 1.1 Tasks in the Smart Grid Cyber Security Strategy

Task 1. Selection of use cases with cyber security considerations.[2]

The use cases were selected from several existing sources, e.g., IntelliGrid, Electric Power Research Institute (EPRI), and Southern California Edison (SCE). The set of use cases provides a common framework for performing the risk assessment, developing the security architecture, and selecting and tailoring the security requirements.

Task 2. Performance of a risk assessment

[2] A use case is a method of documenting applications and processes for purposes of defining requirements.

The risk assessment, including identifying vulnerabilities, impacts, and threats, has been undertaken from a high-level overall functional perspective. The output will be the basis for the selection of security requirements and the identification of security requirements gaps.

Vulnerability classes: the initial draft list of vulnerability classes[3] was developed using information from several existing documents and Web sites, e.g., NIST SP 800-82 and the Open Web Application Security Project (OWASP) vulnerabilities list. These vulnerability classes will ensure that the security controls address the identified vulnerabilities. The vulnerability classes may also be used by Smart Grid implementers, e.g., vendors and utilities, in assessing their systems.

Overall Analysis: both top-down and bottom-up approaches were used in implementing the risk assessment as specified earlier. The top-down approach focuses on the use cases and the overall Smart Grid functionality.

> **Bottom-up analysis:** the bottom-up approach focuses on well-understood problems that need to be addressed, such as authenticating and authorizing users to substation intelligent electronic devices (IEDs), key management for meters, and intrusion detection for power equipment. Also, interdependencies among Smart Grid domains/systems were considered when evaluating the impacts of a cyber or physical security incident. An incident in one infrastructure can cascade to failures in other domains/systems. The bottom-up analysis is included in Appendix D of this document.
>
> **Top-down analysis:** in the top-down approach, logical interface diagrams were developed for the six functional priority areas that were the focus of the initial draft of NISTIR 7628—Electric Transportation, Electric Storage, Wide Area Situational Awareness, Demand Response, Advanced Metering Infrastructure, and Distribution Grid Management. In this draft, a functional architecture for the overall Smart Grid is included, with logical interfaces identified for the additional grid areas (this will be used in the development of the security architecture). Because there are hundreds of interfaces, each logical interface is allocated to one of eighteen logical interface categories. Some examples of the logical interface categories are: control systems with high data accuracy and high availability, as well as media and computer constraints; B2B (Business to Business) connections, interfaces between sensor networks and controls systems; and interface to the customer site. A set of attributes, e.g., immature or proprietary protocols, insecure locations, integrity requirements, was defined, and the attributes allocated to the interface categories, as appropriate. This logical interface category/attributes matrix is used in assessing the impact of a security compromise on confidentiality, integrity and availability. The level of impact is denoted as low, moderate, or high[4]. This assessment is performed for each logical interface category. The output from this process is used in the selection of security requirements (Task 3).

As with any assessment, a realistic analysis of the threats is critical to the overall outcome. The Smart Grid is no different. It is recommended that all organizations take a realistic view of the

[3] A *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. A vulnerability class is a grouping of common vulnerabilities.

[4] The definitions of low, moderate, and high impact are found in FIPS 199.

threats, and work with national authorities as needed to glean the required information, which, it is anticipated, no single utility or other Smart Grid participant would be able to assess on their own. Potential threats range from script-kiddies to disgruntled current or former employees, to nation-state adversaries. A realistic assessment of these threats, and the applicability to subsequent risk-mitigation strategies, is critical to the overall security of the Smart Grid.

Task 3. Specification of high level security requirements.

There are many requirements documents that may be applicable to the Smart Grid. Currently, only NERC Critical Infrastructure Protection (CIP) standards are mandatory for the bulk electric system. The following documents have been identified by members of the SGIP-CSWG as having security requirements relevant to one or more aspects of the Smart Grid.

The following standards are directly relevant to the Smart Grid:

- NERC CIP 002, 003-009
- IEEE 1686-2007, *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*
- *Security Profile for Advanced Metering Infrastructure,* v 1.0, Advanced Security Acceleration Project – Smart Grid, December 10, 2009
- *UtilityAMI Home Area Network System Requirements Specification,* 2008
- IEC 62351 1-8, Power System Control and Associated Communications - Data and Communication Security

The following documents are applicable to control systems:

- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology* and *Part 2: Establishing a Manufacturing and Control Systems Security Program*
- NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009
- NIST SP 800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*, Sept. 2008
- Cyber Security Procurement Language for Control Systems, Version 1.8, Department of Homeland Security, National Cyber Security Division, February 2008
- *Catalog of Control Systems Security: Recommendations for Standards Developers*, Department of Homeland Security, 2009
- ISA SP100, *Wireless Standards*

The cyber security requirements in the documents listed above are not unique. To assist in assessing and selecting the requirements, a cross-reference matrix was developed. This matrix maps the requirements from the various documents listed above. The matrix will be used to select the security requirements that will be listed for each logical interface category. In addition, there are many security requirements that are common to all the logical interface categories. The majority of these requirements are for governance, risk and compliance. These

common requirements will be listed in a separate table, rather than being assigned to each logical interface category. As noted above, these requirements lists are provided as guidance, and are not mandatory. Each organization will need to perform a risk assessment to determine the applicability of the recommended requirements.
In addition, organizations may find it necessary to identify compensating security requirements. A compensating security requirement is implemented by an organization in lieu of a recommended security requirement to provide an equivalent or comparable level of protection for the information/control system and the information processed, stored, or transmitted by that system. More than one compensating requirement may be required to provide the equivalent or comparable protection for a particular security requirement. For example, an organization with significant staff limitations may compensate for the recommended separation of duty security requirement by strengthening the audit, accountability, and personnel security requirements within the information/control system.

Finally, for decades, power system operations have been managing the reliability of the power grid in which power *availability* has been a major requirement, with information integrity as a secondary but increasingly critical requirement. Confidentiality of customer information is also important in the normal revenue billing processes. Although focused on accidental/inadvertent security problems, such as equipment failures, employee errors, and natural disasters, existing power system management technologies can be used and expanded to provide additional security measures.

Privacy Impact Assessment: because the evolving Smart Grid presents potential privacy risks, a privacy impact assessment was performed. Several general privacy principles were used to assess the Smart Grid and findings and recommendations were developed. The results will be used in the identification and tailoring of security requirements.

Task 4a. Development of a security architecture.

As specified in Task 2 above, the first phase in this task is to assess and revise the six functional priority area diagrams. The additional functionality of the Smart Grid will be included in an overall functional architecture that includes the six functional priority areas. This functional architecture will is included in Chapter 2 of this draft.

Using the conceptual model included in this framework document, the FERC priority area use case diagrams, and the additional areas of AMI and distribution grid management, the SGIP-CSWG developed a more granular functional architecture for the Smart Grid. This architecture consolidates the individual diagrams into a single diagram and expands upon the conceptual model. The functional architecture identifies logical communication interfaces between actors. This functional architecture will be submitted to the SGIP Architecture Committee for its use.

In the next phase of this task, the Smart Grid conceptual reference model and the functional architecture will be used in developing a single Smart Grid security architecture. The Smart Grid security architecture will overlay the security requirements on this architecture. The objective is to ensure that cyber security is addressed as a critical cross-cutting requirement of the Smart Grid.

Task 4b. Assessment of Smart Grid standards.

In Task 4b, standards that have been identified as relevant to the Smart Grid by the Priority Action Plan (PAP) teams and the SGIP will be assessed to determine if the security requirements are addressed. In this process, security requirement gaps will be identified and recommendations will be made for addressing the gaps. Also, conflicting standards and standards with security requirements not consistent with the security requirements included in NISTIR 7628 will be identified with recommendations.

Task 5. Conformity Assessment.

The final task is to develop a conformity assessment program for security requirements. This program will be coordinated with the activities defined by the testing and certification standing committee of the Smart Grid Interoperability Panel. This task will be initiated in the spring of 2010.

Several sub-groups were established including Vulnerability Class Analysis, Bottom-up Assessment, Privacy, Standards Assessment, Research and Development, High Level Requirements, and Functional Architecture Development. The final product is being published as NIST Cyber Security Strategy and Requirements Interagency Report 7628 (NISTIR 7628).

SUMMARY OF THE CURRENT STATUS OF THE CHAPTERS AND MAJOR REVISIONS

The key updates and take-aways with this DRAFT of the NISTIR 7628 are highlighted below:

Functional Architecture Development

The functional logical architecture represents a blending of the initial set of use cases and requirements that came from the workshops and the initial NIST Smart Grid Interoperability Roadmap. The architecture group aggregated these six lower level diagrams and consolidated them into a single logical architecture with descriptions of each actor and interface. All of the logical interfaces included in the six diagrams are included in the overall functional logical architecture. This functional logical architecture focuses on a short-term view (1 to 5 years) of the proposed Smart Grid.

Bottom-up Assessment

The Bottom-up Security Analysis sub-group added additional Evident and Specific Cyber Security problems, additional Non-Specific Cyber Security Issues, a new section Design Considerations, and moved and revised some subsections previously in "Non-Specific Cyber Security Issues" to the new "Design Considerations" section. These design considerations discuss important cyber security issues that arise in the design, deployment, and use of smart grid systems, and should be considered by system designers, implementers, purchasers, integrators, and users of smart grid technologies.

Privacy

The focus of the Privacy sub-group has been on what data may be collected or created that can reveal information about individuals or activities within specific premises (both residential and commercial), how these different types of information may be exploited, and policies and practices to identify and mitigate risks. The group conducted a privacy impact assessment (PIA) for the consumer-to-utility portion of the Smart Grid. In the months following the PIA, the group additionally considered the privacy impacts and risks throughout the entire Smart Grid

structure, and also began to conduct an overview of the laws, regulations and standards relevant to the privacy of energy consumption data.

Standards

The Standards sub-group is a new sub-group that added Chapter 5, titled Standards Review. This chapter includes a tabularized view of standards and characteristics that apply to Cyber Security for the Smart Grid. The DHS catalogue was used as an initial source to develop these tables. Currently this chapter presents: an overview of each of the standards currently under review, identification of the security families that are addressed by each standard, identification of the applicable OSI layers addressed by each standard, and a list of notes/comments pertaining to each standard. Additional standards, as found to apply, will be included and reviewed in future versions of this document.

Research and Development (R & D)

The R & D sub-group is another new sub-group that added Chapter 6 titled "Research and Development Themes for Cyber Security in the Smart Grid". The chapter is organized into the following five high level thematic issues requiring immediate research and development: device level, novel mechanisms, systems level, networking issues, and other security issues in the Smart Grid context. The specific topics were based on solicitation from members of the group and from problems that are widely known in the Smart Grid cyber security community. The R & D sub-group will revise and update this chapter by tracking government, academic, and industry R & D efforts that are related to Smart Grid cyber security. Revisions will also be made as new topics are identified from other SGIP-CSWG sub-groups such as bottom-up, vulnerability, and privacy.

Vulnerability Class Analysis

In the latest revision of the vulnerability section, an introduction was added to each of the major categories with clarifying descriptions for the section, and a brief discussion of the intent of the section. There was some minor re-organization of several sections, and some redundant material was removed from the document. Several sections received additional examples, and continued editing. Lastly, comments that were received from interested parties were incorporated into the overall document.

This is very important, transformational work for the electric industry and it is critically important for all stakeholders to be actively engaged to ensure we get interoperability standards that achieve the most potential from Smart Grid technologies without negatively impacting the reliability of the proven technologies we depend on today.

CHAPTER ONE
CYBER SECURITY STRATEGY

With the implementation of the Smart Grid, the information technology (IT) and telecommunications infrastructures have become more important to ensure the reliability and security of the electric sector. Therefore, the security of systems and information in the IT and telecommunications infrastructures must also be addressed by an increasingly diverse electric sector. Security must be included at the design phase to ensure adequate protection.

Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. The need to address potential vulnerabilities has been acknowledged across the federal government, including the National Institute of Standards and Technology (NIST)[5], the Department of Homeland Security (DHS),[6] the Department of Energy (DOE),[7] and the Federal Energy Regulatory Commission (FERC).[8]

Additional risks to the grid include:

- Increasing the complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors;
- Interconnected networks can introduce common vulnerabilities;
- Increasing vulnerabilities to communication disruptions and introduction of malicious software could result in denial of service or compromise the integrity of software and systems;
- Increased number of entry points and paths for potential adversaries to exploit; and
- Potential for compromise of data confidentiality, including the breach of customer privacy.

With the ongoing transition to the Smart Grid, the IT and telecommunication sectors will be more directly involved. These sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in their systems. These same vulnerabilities need to be assessed in the context of the Smart Grid infrastructure. In

[5] Testimony of Cita M. Furlani, Director, Information Technology Laboratory, NIST, before the United States House of Representatives Homeland Security Subcommittee on Emerging Threats, Cyber security, and Science and Technology, March 24, 2009.

[6] Statement for the Record, Sean P. McGurk, Director, Control Systems Security Program, National Cyber Security Division, National Protection and Programs Directorate, Department of Homeland Security, before the U.S. House of Representatives Homeland Security Subcommittee on Emerging Threats, Cyber security, and Science and Technology, March 24, 2009.

[7] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Smart Grid investment Grant Program, Funding Opportunity: DE-FOA-0000058, Electricity Delivery and Energy Reliability Research, Development and Analysis, June 25, 2009.

[8] Federal Energy Regulatory Commission, Smart Grid Policy, 128 FERC ¶ 61,060 [Docket No. PL09-4-000] July 16, 2009.

addition, the Smart Grid will have additional vulnerabilities due to its complexity, large number of stakeholders, and highly time-sensitive operational requirements.

NIST leads a Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG) which now has more than 300 volunteer members from the public and private sectors, academia, regulatory organizations, and federal agencies. Cyber security is being addressed using a thorough process that will result in a comprehensive set of cyber security requirements. As explained more fully later in this chapter, these requirements are being developed (or augmented, where standards/guidelines already exist) using a high-level risk assessment process that is defined in the cyber security strategy for the Smart Grid. Cyber security requirements are implicitly recognized as critical in all of the priority action plans discussed in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* (NIST Special Publication 1108) document that was published January 2010.[9]

1.1 CYBER SECURITY AND THE ELECTRIC SECTOR

The critical role of cyber security in ensuring the effective operation of the Smart Grid is documented in legislation and in the DOE Energy Sector Plan.

Section 1301 of the Energy Independence and Security Act of 2007 (P.L. 110-140) states that, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2. Dynamic optimization of grid operations and resources, with full cyber-security. ...."

Cyber security for the Smart Grid supports both the reliability of the grid and the confidentiality of the information that is transmitted.

DOE's *Energy Sector-Specific Plan*[10] "envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government."

1.2 SCOPE AND DEFINITIONS

The following definition of cyber infrastructure from the National Infrastructure Protection Plan (NIPP) is included to ensure a common understanding.

- **Cyber Infrastructure:** Includes electronic information and communications systems and services and the information contained in these systems and services. Information and

[9] Available at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf.

[10] Department of Energy, *Energy, Critical Infrastructure and Key Resources, Sector-Specific Plan as input to the National Infrastructure Protection Plan*, May 2007

> communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

A traditional IT-focused understanding of cyber security is that it is the protection required to ensure confidentiality, integrity, and availability of the electronic information communication system. For the Smart Grid, this definition of cyber security needs to be more inclusive. Cyber security in the Smart Grid includes both power and cyber system technologies and processes in IT and power system operations and governance. These technologies and processes provide the protection required to ensure confidentiality, integrity, and availability of the Smart Grid cyber infrastructure, including, for example, control systems, sensors, and actuators.

This NIST report provides guidance to organizations that are addressing cyber security for the Smart Grid, e.g., utilities, regulators, power equipment manufacturers and vendors, retail service providers, and electricity and financial market traders. This NIST report provides background information on the analysis process that was used to select and tailor a set of security requirements applicable to the Smart Grid. The process includes both top-down and bottom-up approaches in the selection and tailoring of security requirements for the Smart Grid. The bottom-up approach focuses on identifying vulnerability classes, for example, buffer overflow and protocol errors. The top-down approach focuses on defining components/domains of the Smart Grid system and the logical interfaces between these components/domains. To reduce the complexity, the logical interfaces are organized into logical interface categories. The inter-component/domain security requirements are specified for these logical interface categories based on the interactions between the components and domains. For example, for the AMI system, some of the security requirements are authentication of the meter to the collector, confidentiality for privacy protection, and integrity for firmware updates.

Finally, this NIST report focuses on Smart Grid operations and not on enterprise operations.

1.3 DOCUMENT OVERVIEW

This second draft of NIST Interagency Report (NISTIR) 7628, *Smart Grid Cyber Security Strategy and Requirements*[11] describes the SGIP–CSWG's overall cyber security strategy for the Smart Grid. The cyber security strategy includes a high level risk assessment for the Smart Grid resulting in recommended security requirements. This document includes all the background material that was used in performing the risk assessment and the analysis material used to select the security requirements. In addition, the SGIP-CSWG is reviewing various standards that are included in the NIST Framework document. The review focuses on the security sections of each standard.

[11] The document is available at: http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628. Comments may be submitted to: cswgdraft2comments@nist.gov.

1.3.1 Audience

This document is intended for individuals and organizations who will be addressing cyber security for Smart Grid systems. This includes, for example, vendors, utilities, system operators, researchers and network specialists; and individuals and organizations representing all three sectors –IT, telecommunications, and electric. Individuals reading this document are expected to have a basic knowledge of the electric sector and a basic understanding of cyber security.

1.3.2 Content of the Document

Following is a summary of the content of this document.

- Chapter 1 – *Cyber Security Strategy*: includes background information on the Smart Grid and the importance of cyber security in ensuring the reliability of the Grid and the confidentiality of specific information. It also discusses the cyber security strategy for the Smart Grid and the specific tasks within this strategy.
- Chapter 2 – *Logical Architecture and Interfaces of the Smart Grid*: includes an overall functional logical architecture of the Smart Grid – including all the major domains. This architecture focuses on a short-term view (1-3 years) of the proposed Smart Grid. The chapter also includes individual logical interface diagrams for six areas: electric transportation, electric storage, advanced metering infrastructure (AMI), wide area situational awareness (WASA), distribution grid management, and home area network/business area network (HAN/BAN)[12]. These lower level logical interface diagrams provide a more granular view of the Smart Grid domains. All of the logical interfaces included in the six diagrams are included in the overall functional architecture.
- Chapter 3 – *High Level Security Requirements*: specifies the high level security requirements for the Smart Grid. The supporting documentation that was used to develop the high level security requirements, e.g., logical interface categories and attributes, security compromise impact levels (low, moderate, high) for each logical interface category, and allocation of security requirements to each logical interface category. To simplify the task of specifying security requirements, each logical interface in the diagrams in Chapter 2 was allocated to one of eighteen logical interface categories. The security requirements were specified for each logical interface category.
- Chapter 4– *Privacy and the Smart Grid*: includes a privacy impact assessment for the Smart Grid with a discussion of mitigating factors. The chapter also identifies potential privacy issues with the new capabilities included in the Smart Grid.
- Chapter 5 – *Standards Review*: includes a review of the standards that were identified in the workshops that NIST conducted and others that have been identified through the Priority Action Plan (PAP) process. The identification of the standards and protocol documents that support interoperability of the Smart Grid is a key element of the NIST Framework. All the standards will be reviewed to determine if they include security functionality and if that functionality addresses one or more of the security requirements specified in Chapter 3.

[12] This was previously named Demand Response.

- Chapter 6 – *Research and Development (R&D)*: includes R&D themes that identify where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid.

Also included in this document are several appendixes:

- *Appendix A*: key power system use cases with security applicability used in the risk assessment process
- *Appendix B*: crosswalk of cyber security documents used in developing the security requirements
- *Appendix C*: vulnerability classes used in the risk assessment process
- *Appendix D*: bottom-up security analysis of the Smart Grid used in the risk assessment process
- *Appendix E*: state laws – Smart Grid and electricity delivery regulations
- *Appendix F*: acronyms and glossary
- *Appendix G*: SGIP-CSWG membership.

The requirements included in this NIST report will form the basis for the standards and guidelines developed with coordination by NIST and the SGIP.

1.4 SMART GRID CYBER SECURITY STRATEGY

The overall cyber security strategy for the Smart Grid examines both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The primary goal of the cyber security strategy should be prevention. However, it also requires that a response and recovery strategy be developed in the event of a cyber attack on the electric system.

Implementation of a cyber security strategy requires the definition and implementation of an overall cyber security risk assessment process for the Smart Grid. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. This type of risk is one component of organizational risk. Organizational risk can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk, and the risk from information systems). The Smart Grid risk assessment process is based on existing risk assessment approaches developed by both the private and public sectors and includes identifying impact, vulnerability, and threat information to produce an assessment of risk to the Smart Grid and to its domains and sub-domains, such as homes and businesses. Because the Smart Grid includes systems from the IT, telecommunications, and energy sectors, the risk assessment process is applied to all three sectors as they interact in the Smart Grid.

The following documents were used in developing the risk assessment for the Smart Grid:

- Special Publication (SP) 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective*, NIST, April 2008;
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems,* NIST, March 2006;

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, NIST, February 2004;
- *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, North American Electric Reliability Corporation (NERC), 2002;
- *The National Infrastructure Protection Plan, Partnering to enhance protection and resiliency***,** Department of Homeland Security, 2009;
- The IT, telecommunications, and energy sectors sector-specific plans (SSPs), initially published in 2007 and updated annually;
- ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems: Concepts, Terminology and Models*, International Society of Automation (ISA), 2007; and
- ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, ISA, January 2009.

Following the risk assessment, the next step in the Smart Grid cyber security strategy is to select and tailor (as necessary) the security requirements. The documents used in this step are listed under Task 3 below.

The security requirements and the supporting analysis that are included in this NIST report may be used by implementers of the Smart Grid, e.g., utilities, equipment manufacturers, regulators, as input to their risk assessment processes. The information serves as baseline guidance to the various organizations for assessing risk and selecting appropriate security requirements. In addition, each organization should develop its own cyber security strategy for the Smart Grid.

The tasks within the cyber security strategy for the Smart Grid are undertaken by participants in the SGIP-CSWG[13]. In addition, the SGIP-CSWG is coordinating activities with the Advanced Security Acceleration Project – Smart Grid (ASAP-SG). The ASAP-SG is a collaborative effort between EnerNex Corporation, multiple major North American utilities, NIST, and DOE, including resources from Oak Ridge National Laboratory and the Software Engineering Institute of Carnegie Mellon University. Following are the tasks that are being performed by the SGIP-CSWG in the implementation of the cyber security strategy. Also included are the deliverables for each task. Because of the time frame for developing the document, the tasks listed below are occurring in parallel, with significant interactions among the groups addressing the tasks.

Figure 1.1 illustrates the tasks defined for the Smart Grid cyber security strategy. The tasks are defined after the figure.

[13] The SGIP–CSWG was formerly known as the Cyber Security Coordination Task Group (CSCTG). The CSWG was established as a permanent working group within the SGIP.

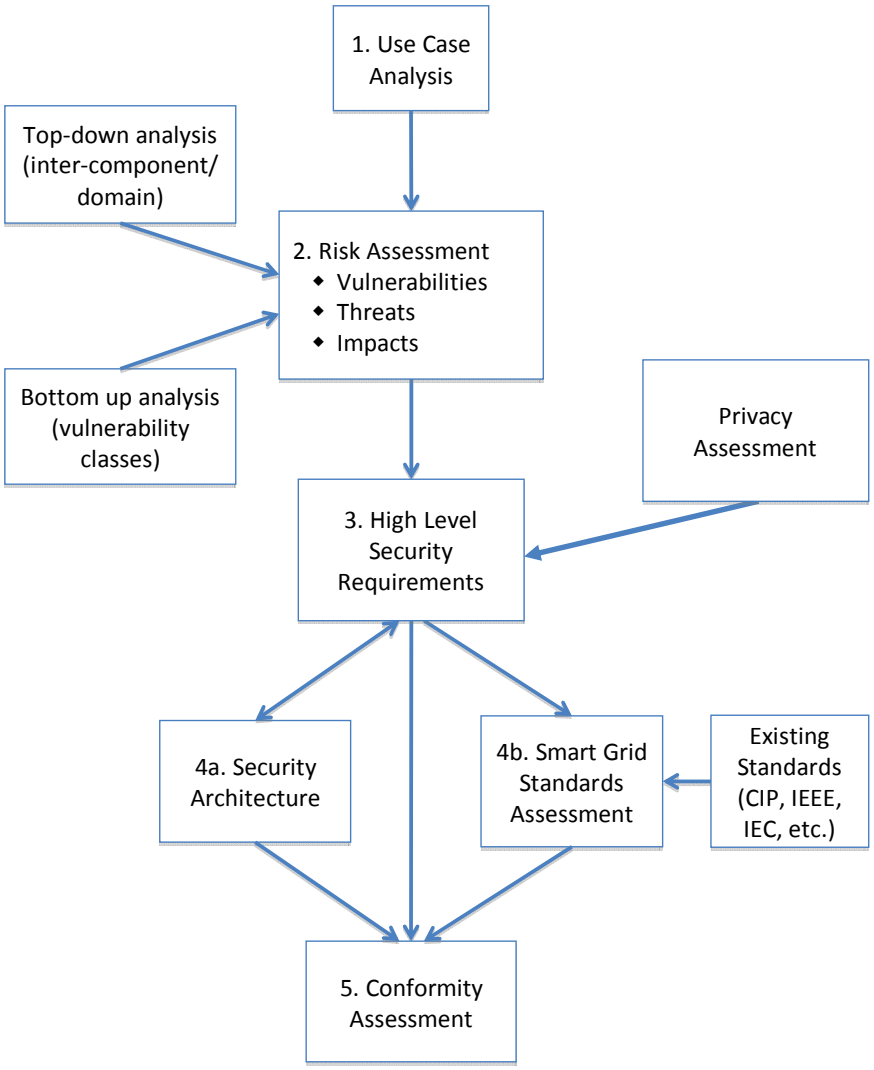

Figure 1.1 Tasks in the Smart Grid Cyber Security Strategy

Task 1. Selection of use cases with cyber security considerations.[14]

The use cases were selected from several existing sources, e.g., IntelliGrid, Electric Power Research Institute (EPRI), and Southern California Edison (SCE). The set of use cases provides a common framework for performing the risk assessment, developing the security architecture, and selecting and tailoring the security requirements.

Task 2. Performance of a risk assessment

The risk assessment, including identifying vulnerabilities, impacts, and threats, has been undertaken from a high-level overall functional perspective. The output will be the basis for the selection of security requirements and the identification of security requirements gaps.

Vulnerability classes: the initial draft list of vulnerability classes[15] was developed using information from several existing documents and Web sites, e.g., NIST SP 800-82 and the Open

[14] A use case is a method of documenting applications and processes for purposes of defining requirements.

Web Application Security Project (OWASP) vulnerabilities list. These vulnerability classes will ensure that the security controls address the identified vulnerabilities. The vulnerability classes may also be used by Smart Grid implementers, e.g., vendors and utilities, in assessing their systems.

Overall Analysis: both top-down and bottom-up approaches were used in implementing the risk assessment as specified earlier. The top-down approach focuses on the use cases and the overall Smart Grid functionality.

> **Bottom-up analysis:** the bottom-up approach focuses on well-understood problems that need to be addressed, such as authenticating and authorizing users to substation intelligent electronic devices (IEDs), key management for meters, and intrusion detection for power equipment. Also, interdependencies among Smart Grid domains/systems were considered when evaluating the impacts of a cyber or physical security incident. An incident in one infrastructure can cascade to failures in other domains/systems. The bottom-up analysis is included in Appendix D of this document.
>
> **Top-down analysis:** in the top-down approach, logical interface diagrams were developed for the six functional priority areas that were the focus of the initial draft of NISTIR 7628—Electric Transportation, Electric Storage, Wide Area Situational Awareness, Demand Response, Advanced Metering Infrastructure, and Distribution Grid Management. In this draft, a functional architecture for the overall Smart Grid is included, with logical interfaces identified for the additional grid areas (this will be used in the development of the security architecture). Because there are hundreds of interfaces, each logical interface is allocated to one of eighteen logical interface categories. Some examples of the logical interface categories are: control systems with high data accuracy and high availability, as well as media and computer constraints; B2B (Business to Business) connections; interfaces between sensor networks and controls systems; and interface to the customer site. A set of attributes (e.g., immature or proprietary protocols, insecure locations, integrity requirements) was defined, and the attributes allocated to the interface categories, as appropriate. This logical interface category/attributes matrix is used in assessing the impact of a security compromise on confidentiality, integrity and availability. The level of impact is denoted as low, moderate, or high[16]. This assessment is performed for each logical interface category. The output from this process is used in the selection of security requirements (Task 3).

As with any assessment, a realistic analysis of the threats is critical to the overall outcome. The Smart Grid is no different. It is recommended that all organizations take a realistic view of the threats, and work with national authorities as needed to glean the required information, which, it is anticipated, no single utility or other Smart Grid participant would be able to assess on its own. Potential threats range from script-kiddies to disgruntled current or former employees, to nation-state adversaries. A realistic assessment of these threats, and the applicability to subsequent risk-mitigation strategies, is critical to the overall security of the Smart Grid.

---

[15] A *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. A vulnerability class is a grouping of common vulnerabilities.

[16] The definitions of low, moderate, and high impact are found in FIPS 199.

Task 3. Specification of high level security requirements.

There are many requirements documents that may be applicable to the Smart Grid. Currently, only NERC Critical Infrastructure Protection (CIP) standards are mandatory for the bulk electric system. The following documents have been identified by members of the SGIP-CSWG as having security requirements relevant to one or more aspects of the Smart Grid.

The following standards are directly relevant to the Smart Grid:

- NERC CIP 002, 003-009, version 3
- IEEE 1686-2007, *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*
- *Security Profile for Advanced Metering Infrastructure,* v 1.0, Advanced Security Acceleration Project – Smart Grid, December 10, 2009
- *UtilityAMI Home Area Network System Requirements Specification,* 2008
- IEC 62351 1-8, Power System Control and Associated Communications - Data and Communication Security

The following documents are applicable to control systems:

- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology* and *Part 2: Establishing a Manufacturing and Control Systems Security Program*
- NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009
- NIST SP 800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*, Sept. 2008
- Cyber Security Procurement Language for Control Systems, Version 1.8, Department of Homeland Security, National Cyber Security Division, February 2008
- *Catalog of Control Systems Security: Recommendations for Standards Developers*, Department of Homeland Security, 2009
- ISA SP100, *Wireless Standards*

The cyber security requirements in the documents listed above are not unique. To assist in assessing and selecting the requirements, a cross-reference matrix was developed. This matrix maps the requirements from the various documents listed above. The matrix will be used to select the security requirements that will be listed for each logical interface category. In addition, there are many security requirements that are common to all the logical interface categories. The majority of these requirements are for governance, risk and compliance. These common requirements will be listed in a separate table, rather than being assigned to each logical interface category. As noted above, these requirements lists are provided as guidance, and are not mandatory. Each organization will need to perform a risk assessment to determine the applicability of the recommended requirements.

In addition, organizations may find it necessary to identify compensating security requirements. A compensating security requirement is implemented by an organization in lieu of a recommended security requirement to provide an equivalent or comparable level of protection for the information/control system and the information processed, stored, or transmitted by that system. More than one compensating requirement may be required to provide the equivalent or comparable protection for a particular security requirement. For example, an organization with significant staff limitations may compensate for the recommended separation of duty security requirement by strengthening the audit, accountability, and personnel security requirements within the information/control system.

Finally, for decades, power system operations have been managing the reliability of the power grid in which power *availability* has been a major requirement, with information integrity as a secondary but increasingly critical requirement. Confidentiality of customer information is also important in the normal revenue billing processes. Although focused on accidental/inadvertent security problems, such as equipment failures, employee errors, and natural disasters, existing power system management technologies can be used and expanded to provide additional security measures.

Privacy Impact Assessment: because the evolving Smart Grid presents potential privacy risks, a privacy impact assessment was performed. Several general privacy principles were used to assess the Smart Grid and findings and recommendations were developed. The results will be used in the identification and tailoring of security requirements.

Task 4a. Development of a security architecture.

As specified in Task 2 above, the first phase in this task is to assess and revise the six functional priority area diagrams. The additional functionality of the Smart Grid will be included in an overall functional architecture that includes the six functional priority areas. This functional architecture is included in Chapter 2 of this draft.

Using the conceptual model included in this framework document, the FERC priority area use case diagrams, and the additional areas of AMI and distribution grid management, the SGIP-CSWG developed a more granular functional architecture for the Smart Grid. This architecture consolidates the individual diagrams into a single diagram and expands upon the conceptual model. The functional architecture identifies logical communication interfaces between actors. This functional architecture will be submitted to the SGIP Architecture Committee for its use.

In the next phase of this task, the Smart Grid conceptual reference model and the functional architecture will be used in developing a single Smart Grid security architecture. The Smart Grid security architecture will overlay the security requirements on this architecture. The objective is to ensure that cyber security is addressed as a critical cross-cutting requirement of the Smart Grid.

Task 4b. Assessment of Smart Grid standards.

In Task 4b, standards that have been identified as relevant to the Smart Grid by the Priority Action Plan (PAP) teams and the SGIP will be assessed to determine if the security requirements are addressed. In this process, security requirement gaps will be identified and recommendations will be made for addressing the gaps. Also, conflicting standards and standards with security

requirements not consistent with the security requirements included in NISTIR 7628 will be identified with recommendations.

Task 5. Conformity Assessment.

The final task is to develop a conformity assessment program for security requirements. This program will be coordinated with the activities defined by the testing and certification standing committee of the Smart Grid Interoperability Panel. This task will be initiated in the spring of 2010.

1.5 TIME LINE

This second draft of NISTIR 7628 addresses the comments that were submitted in response to the first public draft and is being posted for public review and comment for 60 days.[17] The final first version of NISTIR 7628, scheduled to be published in spring of 2010, will address all comments submitted to date, and will include updated sections of the current document, an overall security architecture, and design considerations to assist individuals and organizations in using the document. Because the Smart Grid is evolving over time, the content of NISTIR 7628 will need to be reviewed and updated, as required.

[17] Comments may be submitted to: cswgdraft2comments@nist.gov

CHAPTER TWO
LOGICAL ARCHITECTURE AND INTERFACES OF THE SMART GRID

This chapter includes an overall functional logical architecture of the Smart Grid – including all the major domains: service providers, customer, transmission, distribution, bulk generation, markets and operations that are part of the NIST conceptual model. Figure 2.1 is this high level functional architecture and represents a composite high level view of Smart Grid domains and actors. A Smart Grid domain is a high-level grouping of organizations, buildings, individuals, systems, devices or other *actors* with similar objectives and relying on – or participating in – similar types of applications. Communications among actors in the same domain may have similar characteristics and requirements. Domains may contain sub-domains. Moreover, domains have much overlapping functionality, as in the case of the transmission and distribution domains. An *actor* is a device, computer system, software program, or the individual or organization that participates in the Smart Grid. Actors have the capability to make decisions and to exchange information with other actors. Organizations may have actors in more than one domain. The actors illustrated here are representative examples, and are not all the actors in the Smart Grid. Each of the actors may exist in several different varieties, and may contain many other actors within them.

The functional logical architecture represents a blending of the initial set of use cases and requirements that came from the workshops and the initial NIST Smart Grid Interoperability Roadmap, including the individual logical interface diagrams for the six application areas: electric transportation, electric storage, advanced metering infrastructure (AMI), wide area situational awareness (WASA), distribution grid management, and home area network/business area network (HAN/BAN)[18]. These six areas are depicted in individual diagrams, Figures 2.2 through 2.7. These lower level diagrams were originally produced at the NIST Smart Grid workshops and then revised for this NIST report. They provide a more granular view of the Smart Grid functional areas.

To develop the high level functional logical architecture, the six lower level diagrams were aggregated and consolidated into a single logical architecture. All of the logical interfaces included in the six diagrams are included in the overall functional architecture. The format for the reference number for each logical interface is U99 – where U stands for universal and 99 is the interface number. The reference number is the same on the individual logical diagrams and the functional logical architecture. This functional architecture focuses on a short-term view (1-3 years) of the proposed Smart Grid.

The functional logical architecture is a work in progress and will be subject to revision and further development. Additional underlying detail as well as additional Smart Grid functions will be needed to enable more detailed analysis of required security functions. The graphic

[18] This was previously named Demand Response.

illustrates, at a high level, the diversity of systems as well as a first representation of associations between systems and components of the Smart Grid.

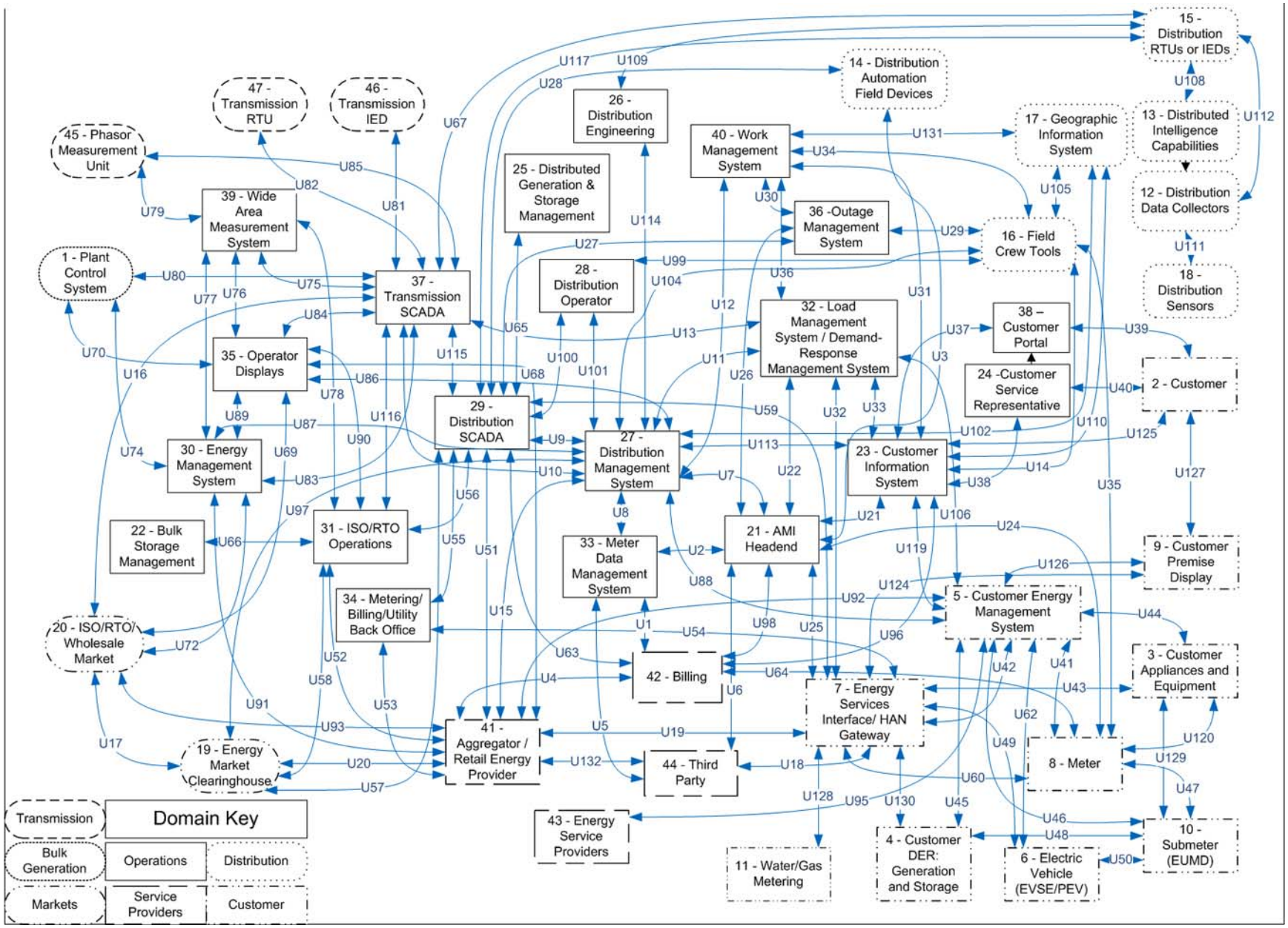

Figure 2.1 Unified Logical Architecture for the Smart Grid

Table 2.1 Actor Descriptions for the Unified Logical Architecture for the Smart Grid

Actor Number	Domain	Actor	Acronym	Description
1.	Bulk Generation	Plant Control System - Distributed Control System	DCS	A local control system at a bulk generation plant. This is sometimes called a Distributed Control System (DCS).
2.	Customer	Customer		An entity that pays for electrical goods or services. A customer of a utility, including customers who provide more power than they consume.
3.	Customer	Customer Appliances and Equipment		A device or instrument designed to perform a specific function, especially an electrical device, such as a toaster, for household use. An electric appliance or machinery that may have the ability to be monitored, controlled and/or displayed.
4.	Customer	Customer Distributed Energy Resources: Generation and Storage	DER	Energy generation resources, such as solar or wind, used to generate and store energy (located on a customer site) to interface to the controller (HAN/BAN) to perform an energy related activity.
5.	Customer	Customer Energy Management System	EMS	An application service that communicates with devices in the home. The application service may have interfaces to the meter to report usage or to the operations domain to get pricing or other information to make automated or manual decisions to control energy consumption more efficiently. The EMS may be a utility subscription service, a consumer written application, or a manual control by the utility or consumer.
6.	Customer	Electric Vehicle Service Element/Plug-in Electric Vehicle	EVSE/PEV	A vehicle driven entirely by an electric motor powered by a rechargeable battery that may be recharged by plugging into the grid or by recharging from a gasoline-driven alternator
7.	Customer	Energy Services Interface/Home Area Network Gateway	HAN	An interface between the distribution, operations, and customer domains and the devices within the customer domain.
8.	Customer	Meter		Utility owned point of sale device used for the transfer of product and measuring usage from one domain/system to another.

Actor Number	Domain	Actor	Acronym	Description
9.	Customer	Customer Premise Display		This device will enable customers to view their usage and cost data within their home or business.
10.	Customer	Sub-Meter - Energy Usage Metering Device	EUMD	A meter connected after the main billing meter. It may or may not be a billing meter and is typically used for information monitoring purposes.
11.	Customer	Water/Gas Metering		Utility owned point of sale device used for the transfer of product (water and gas) and measuring usage from one domain/system to another.
12.	Distribution	Distribution Data Collector		A data concentrator bringing data from multiple sources and putting it into different form factors.
13.	Distribution	Distributed Intelligence Capabilities		Advanced automated/intelligent application from the centralized control system used to increased reliability and responsiveness.
14.	Distribution	Distribution Automation Field Devices		Multi-featured installations meeting a broad range of control, operations, measurements for planning and system performance reports for the utility personnel.
15.	Distribution	Distribution Remote Terminal Unit/Intelligent Electronic Device	RTUs or IEDs	Receive data from sensors and power equipment, and can issue control commands, such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level.
16.	Distribution	Field Crew Tools		A field engineering and maintenance tool set that includes any mobile computing and hand held devices.
17.	Distribution	Geographic Information System	GIS	A spatial asset management system that provides utilities with asset information and network connectivity for advanced applications.
18.	Distribution	Distribution Sensor		A device that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument
19.	Marketing	Energy Market Clearinghouse		Wide-area energy market operation system providing high-level market signals for distribution companies (ISO/RTO and Utility Operations). The control is a financial system, not in the sense

Actor Number	Domain	Actor	Acronym	Description
				of SCADA.
20.	Marketing	Independent System Operator/Regional Transmission Organization Wholesale Market	ISO/RTO	An ISO/RTO control center that participates in the market and does not run the market. From the EPSA web site, "The electric wholesale market is open to anyone who, after securing the necessary approvals, can generate power, connect to the grid and find a counterparty willing to buy their output. These include competitive suppliers and marketers that are affiliated with utilities, independent power producers (IPPs) not affiliated with a utility, as well as some excess generation sold by traditional vertically integrated utilities. All these market participants compete with each other on the wholesale market."[19]
21.	Operations	Advanced Metering Infrastructure Headend	AMI	This system manages the information exchanges between third party systems or systems not considered headend, such as the MDMS system and the AMI network.
22.	Operations	Bulk Storage Management		Energy storage connected to the bulk power system
23.	Operations	Customer Information System	CIS	Enterprise-wide software applications that allow companies to manage aspects of their relationship with a customer.
24.	Operations	Customer Service Representative	CSR	Customer service provided by a person (e.g., sales and service representative), or by automated means called self-service (e.g., Interactive Voice Response (IVR)).

[19] http://www.epsa.org/industry/primer/?fa=wholesaleMarket

Actor Number	Domain	Actor	Acronym	Description
25.	Operations	Distributed Generation and Storage management		Distributed generation, also called on-site generation, dispersed generation, embedded generation, decentralized generation, decentralized energy or distributed energy, generates electricity from many small energy sources and/or stores on dispersed, small devices or systems.
26.	Operations	Distribution Engineering		A technical function of planning and managing the design and upgrading of the distribution system. For example the addition of new customers, the build out for new load, the configuration and/or capital investments for improving system reliability.
27.	Operations	Distribution Management Systems	DMS	A suite of application software that supports electric system operations. Example applications include topology processor, on-line three-phase unbalanced distribution power flow, contingency analysis, study mode analysis, switch order management, short-circuit analysis, volt/VAR management, and loss analysis. These applications provide operations staff and engineering personnel additional information and tools to help accomplish their objectives.
28.	Operations	Distribution Operator		Person operating the distribution grid
29.	Operations	Distribution Supervisory Control and Data Acquisition	SCADA	A distribution SCADA system stores (database) information on devices, distribution feeder parameters, bulk supply interface points, and customer meter connectivity.
30.	Operations	Energy Management System	EMS	A system of computer-aided tools used by operators of electric utility grids to monitor, control, and optimize the performance of the generation and/or transmission system. The monitor and control functions are known as SCADA; the optimization packages are often referred to as "advanced applications". (Note: gas and water could be separate from or integrated within the EMS.)
31.	Operations	ISO/RTO Operations		Wide-area power system control center providing high-level load management and security analysis for the transmission grid, typically using an Energy Management System with generation applications and network analysis applications.

Actor Number	Domain	Actor	Acronym	Description
32.	Operations	Load Management Systems/Demand Response Management System	LMS / DRMS	An LMS issues load management commands to appliances and equipment at customer locations in order to decrease load during peak or emergency situations. The DRMS issues pricing or other signals to appliances and equipment at customer locations in order to request customers (or their pre-programmed systems) to decrease or increase their loads in response to the signals.
33.	Operations	Meter Data Management System	MDMS	System that stores meter data (e.g. energy usage, energy generation, meter logs, meter test results) and makes data available to authorized systems. This system is a component of the customer communication system. This could be called a 'billing meter'.
34.	Operations	Metering/Billing /Utility Back Office		Back office utility systems for metering and billing.
35.	Operations	Operator Displays		This is the human machine interface for the operations systems.
36.	Operations	Outage Management System	OMS	An OMS is a computer system used by operators of electric distribution systems to assist in outage identification and restoration of power. Major functions usually found in an OMS include: • Listing all customers who have outages • Prediction of location of fuse or breaker that opened upon failure. • Prioritizing restoration efforts and managing resources based upon criteria such as locations of emergency facilities, size of outages, and duration of outages. • Providing information on extent of outages and number of customers impacted to management, media and regulators. • Calculation of estimation of restoration times. • Management of crews assisting in restoration. • Calculation of crews required for restoration.
37.	Operations	Transmission SCADA		Transmits individual device status, manages energy consumption by controlling compliant devices, and allows operators to directly control power system equipment.

Actor Number	Domain	Actor	Acronym	Description
38.	Operations	Customer Portal		A computer that delivers (serves up) Web pages. Every Web server has an IP address and possibly a domain name. A utility provided web server where the customer can view their energy and cost information online, enroll in prepayment electric services and enable third party monitoring and control of customer equipment.
39.	Operations	Wide Area Measurement System	WAMS	Communication system that monitors phase measurements and substation equipment over a large geographical base that can use visualization and other techniques to provide system information to power system operators
40.	Operations	Work Management System	WMS	A system that provides project details and schedules for work crews to construct and maintain the power system infrastructure.
41.	Service Provider	Aggregator		Any marketer, broker, public agency, city, county, or special district that combines the loads of multiple end-use customers in facilitating the sale and purchase of electric energy, transmission, and other services on behalf of these customers.
42.	Service Provider	Billing		Process of generating an invoice to recover sales price from the customer.
43.	Service Provider	Energy Service Providers	ESP	Provides retail electricity, natural gas and clean energy options, along with energy efficiency products and services.
44.	Service Provider	Third Party		A third party providing a critical business function outside of the utility.
45.	Transmission	Phasor Measurement Unit	PMU	Measures the electrical waves on an electricity grid to determine the health of the system.
46.	Transmission	Transmission IED		IEDs receive data from sensors and power equipment, and can issue control commands, such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level. A device that sends data to a data concentrator for potential reformatting.

Actor Number	Domain	Actor	Acronym	Description
47.	Transmission	Transmission RTU		RTUs pass status and measurement information from a substation or feeder equipment to a SCADA system, and transmit control commands from the SCADA system to the field equipment.

The following diagrams include detailed logical interfaces. Following each diagram is a table that allocates the logical interfaces to one of the logical interface categories. These logical interface categories are discussed fully in Chapter Three.

2.1 ADVANCED METERING INFRASTRUCTURE (AMI)

Advanced metering infrastructure (AMI) consists of the communications hardware and software and associated system and data management software that creates a two-way network between advanced meters and utility business systems, enabling collection and distribution of information to customers and other parties, such as competitive retail suppliers or the utility itself. AMI provides customers real-time (or near real-time) pricing of electricity and it can help utilities achieve necessary load reductions.

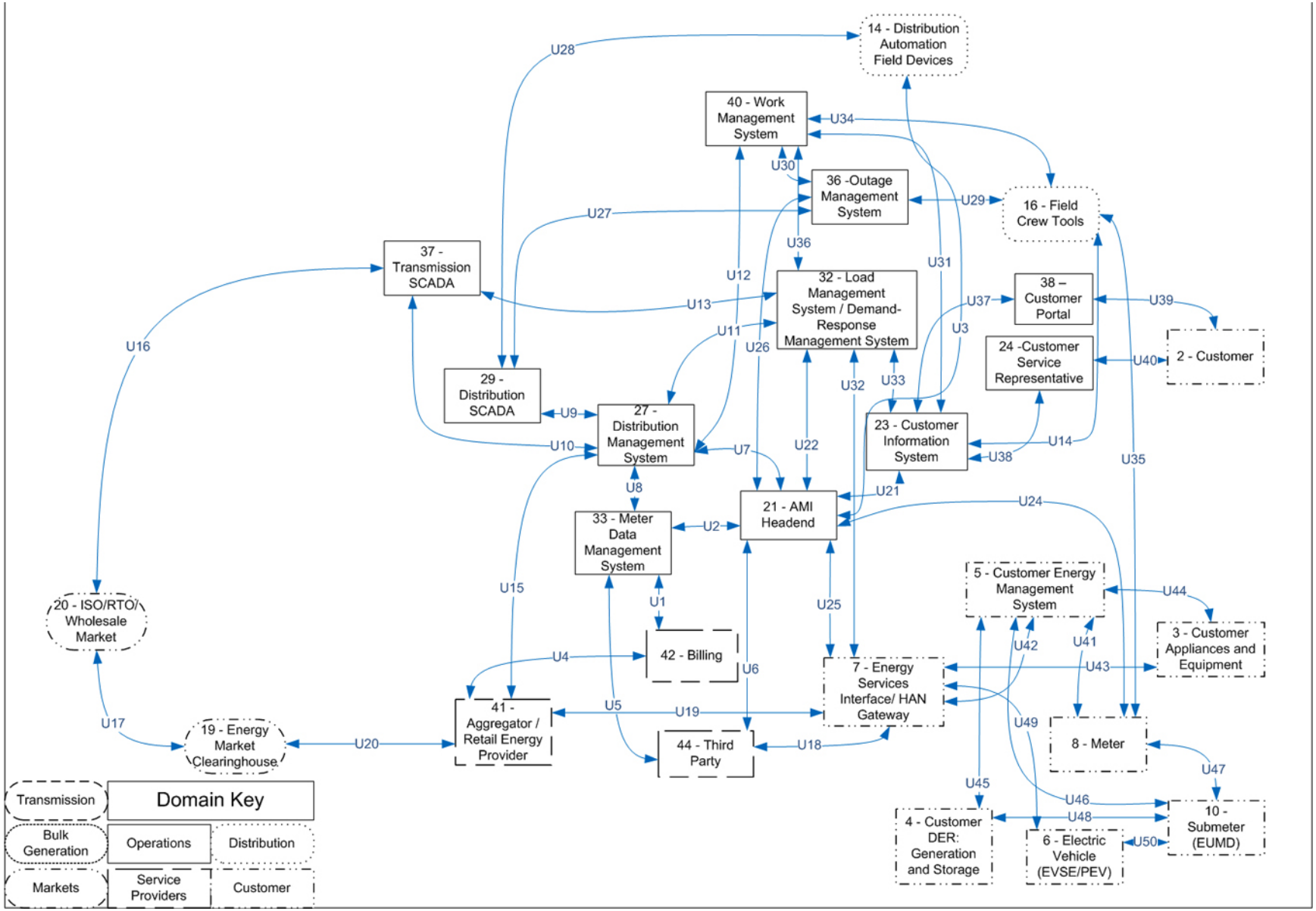

Figure 2.2 Advanced Metering Infrastructure (AMI)

Table 2.2 AMI Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1a. 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	U3, U28
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
1c. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
1d. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
2a. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	U9, U27
2b. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U7, U10, U13, U16
3a. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U4, U22, U26, U31

Logical Interface Category	Logical Interfaces
3b. Interface between back office systems not under common management authority, for example: • Between a third party billing system and a utility meter data management system	U1, U6, U15
6. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U17, U20
7. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U12, U30, U33, U36
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None
9. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
10a. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U8, U21, U25, U32
10b. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs, for example: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U43, U44, U45, U49

Logical Interface Category	Logical Interfaces
12. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U18, U19, U37, U38, U39, U40, U42
13. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U14, U29, U34, U35
14. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41, U46, U47, U50
15. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
16. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	U11
17. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	U5, U132
18. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

2.2 DISTRIBUTION GRID MANAGEMENT (DGM)

Distribution grid management (DGM) focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations. As Smart Grid capabilities, such as AMI and demand response, are developed, and as large numbers of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system. The anticipated benefits of distribution grid management include increased reliability, reductions in peak loads and improved capabilities for managing distributed sources of renewable energy.

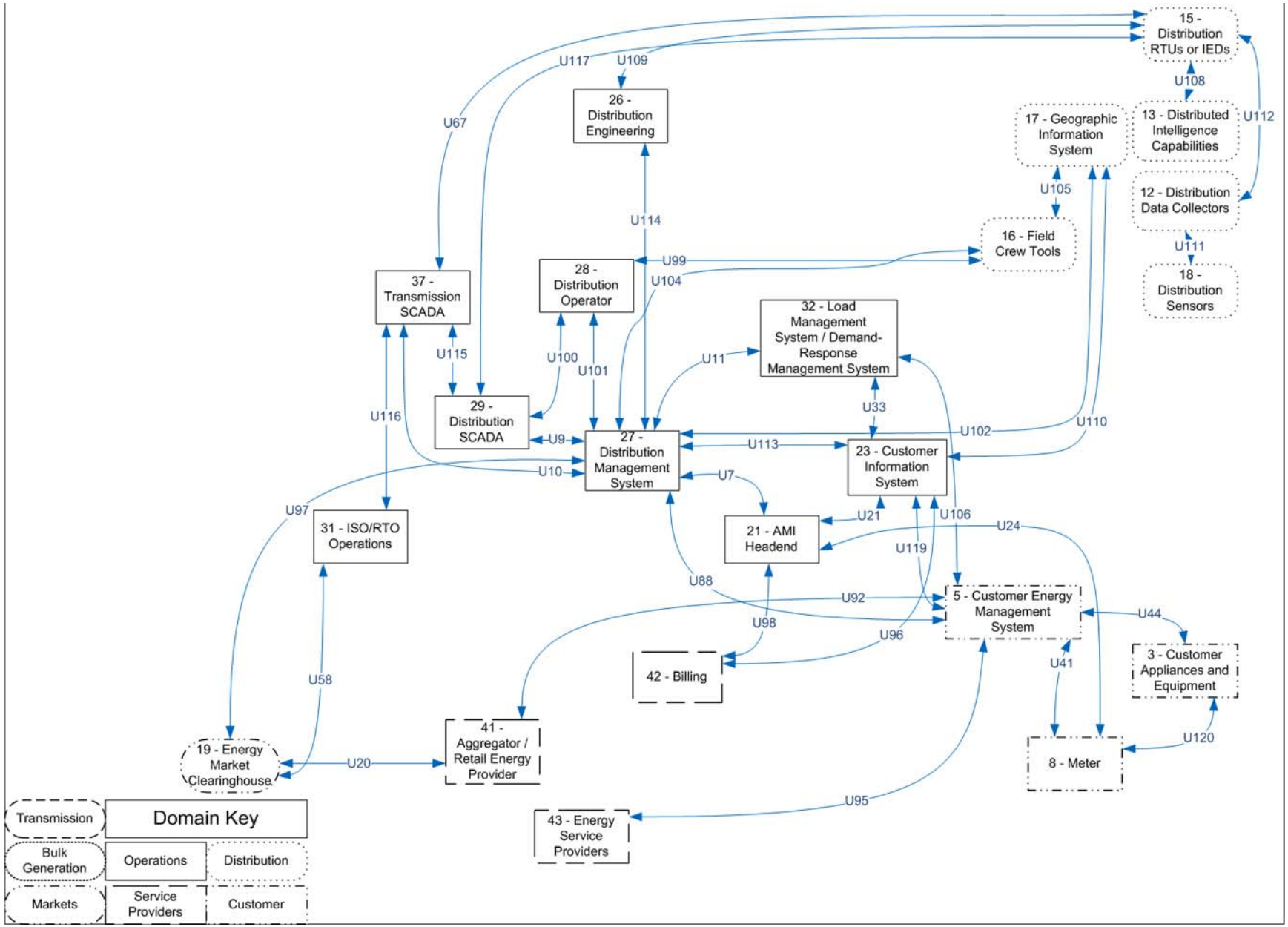

Figure 2.3 Distribution Grid Management (DGM)

Table 2.3 – DGM Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1a. 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	U102, U117
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
1c. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
1d. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
2a. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	U9, U11, U67
2b. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U7, U10, U115, U116
3a. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U21, U96, U98, U110

Logical Interface Category	Logical Interfaces
3b. Interface between back office systems not under common management authority, for example: • Between a third party billing system and a utility meter data management system	None
6. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U20, U58, U97
7. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U33, U106, U113, U114, U131
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	U111
9. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	U108, U112
10a. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U95, U119
10b. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs, for example: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U44, U120

Logical Interface Category	Logical Interfaces
12. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U88, U92, U100, U101
13. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U99, U104, U105
14. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41
15. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
16. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	U109
17. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
18. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

2.3 ELECTRIC STORAGE (ES)

Electric storage (ES) is the means of storing energy, directly or indirectly. The significant bulk of energy storage technology available today is pumped hydro-electric storage hydroelectric technology. New storage capabilities—especially for distributed storage—would benefit the entire grid, from generation to end use.

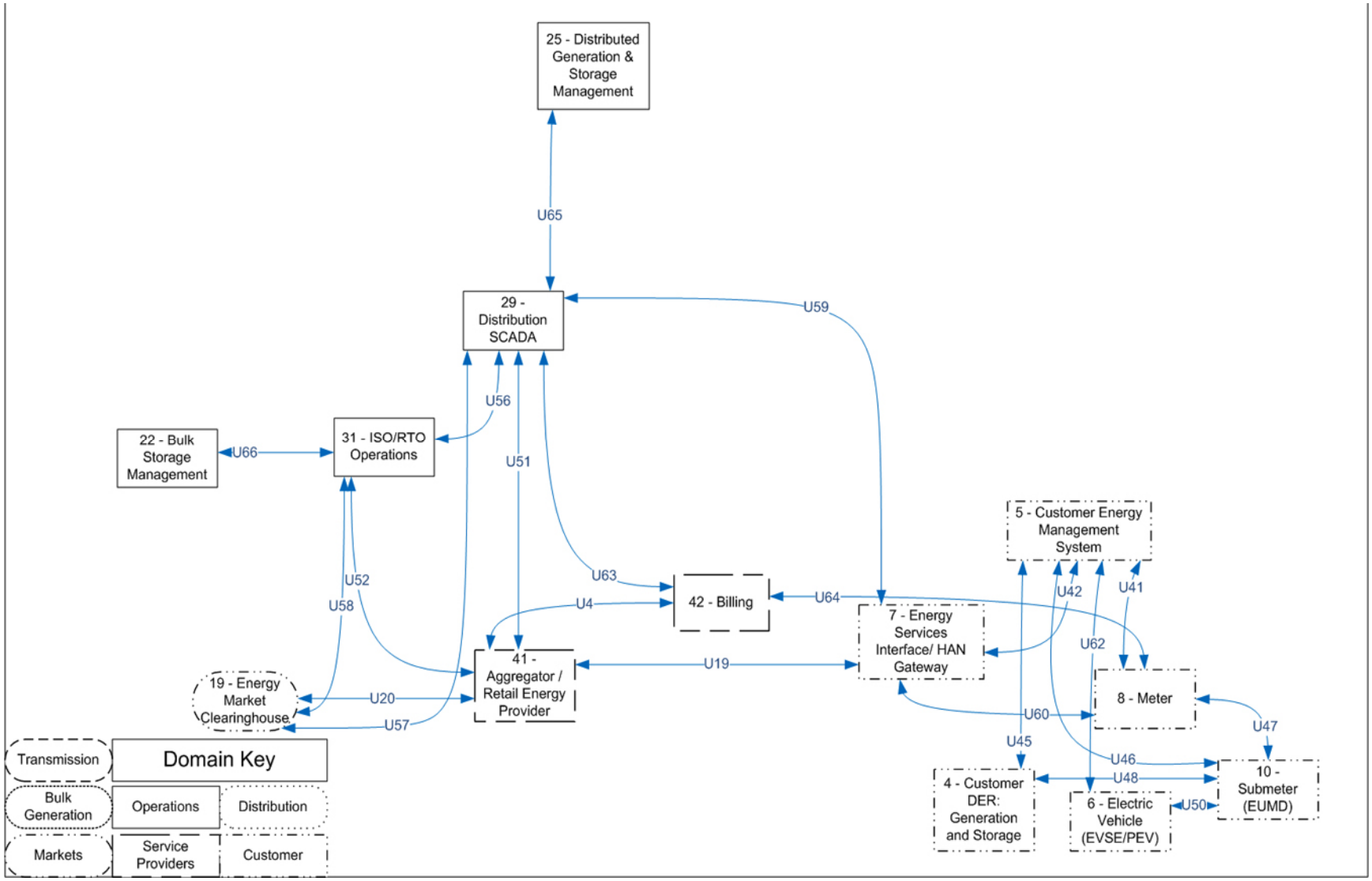

Figure 2.4 Electric Storage (ES)

Table 2.4 – Electric Storage Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1a. 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	None
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
1c. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
1d. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
2a. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	U65, U66
2b. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U56
3a. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U63

Logical Interface Category	Logical Interfaces
3b. Interface between back office systems not under common management authority, for example: • Between a third party billing system and a utility meter data management system	U52
6. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U4, U20, U51, U57, U58
7. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U59
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None
9. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
10a. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U60
10b. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs, for example: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U42, U45, U62

Logical Interface Category	Logical Interfaces
12. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U19
13. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
14. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U41, U46, U47, U48, U50, U64
15. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
16. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	None
17. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
18. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

2.4 ELECTRIC TRANSPORTATION (ET)

Electric transportation (ET) refers primarily to enabling large-scale integration of plug-in electric vehicles (PEVs). Electric transportation could significantly reduce U.S. dependence on foreign oil, increase the use of renewable sources of energy, and dramatically reduce the nation's carbon footprint.

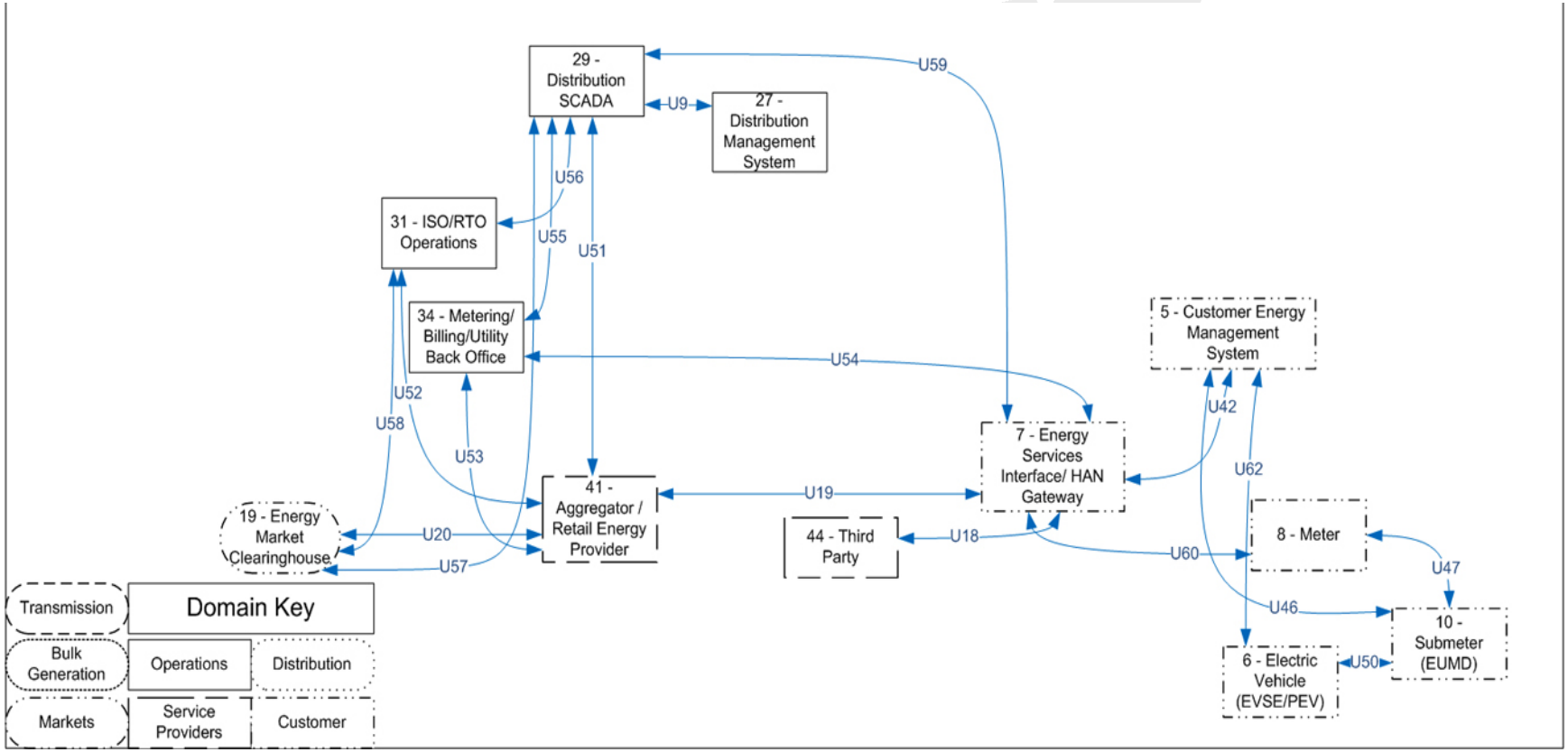

Figure 2.5 Electric Transportation

Table 2.5 – Electric Transportation Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1a. 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	None
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
1c. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
1d. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
2a. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	None
2b. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U56
3a. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	None

Logical Interface Category	Logical Interfaces
3b. Interface between back office systems not under common management authority, for example: • Between a third party billing system and a utility meter data management system	U55
6. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U9, U20, U51, U52, U53, U57, U58
7. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U59
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None
9. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
10a. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	None
10b. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs, for example: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U62

Logical Interface Category	Logical Interfaces
12. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U18, U19, U42
13. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
14. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U46, U47, U50, U53, U54, U60
15. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
16. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	None
17. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
18. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

2.5 HOME AREA NETWORK/BUSINESS AREA NETWORK (HAN/BAN)[20]

The home area network/business area network (HAN/BAN) address demand response and consumer energy efficiency. This includes mechanisms and incentives for utilities, business, industrial, and residential customers to cut energy use during times of peak demand or when power reliability is at risk. Demand response is necessary for optimizing the balance of power supply and demand.

[20] HAN/BAN Network is demand response (DR) in the NIST Framework.

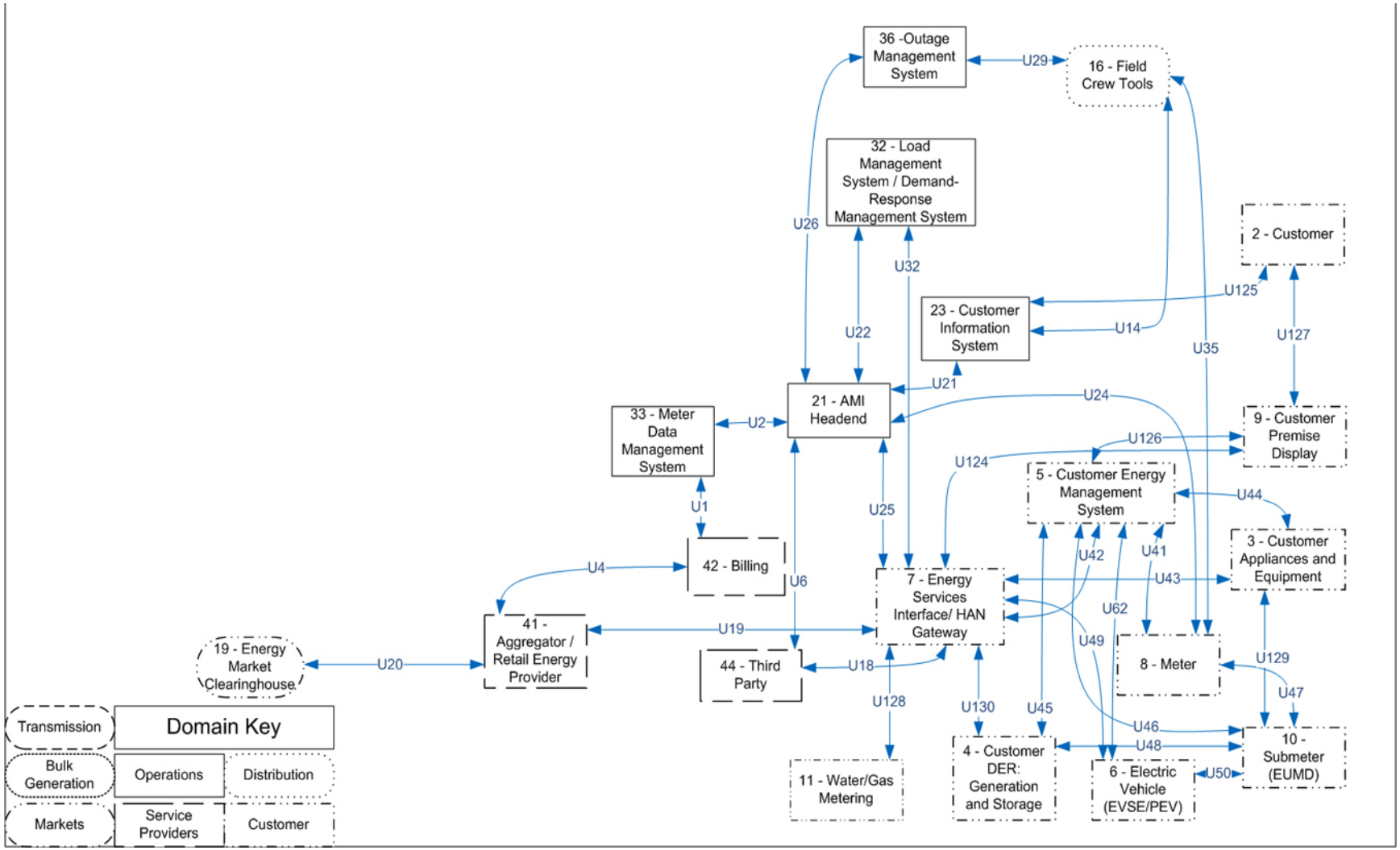

Figure 2.6 Home Area Network/Business Area Network (HAN/BAN)

Table 2.6 – HAN/BAN Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1a. 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	None
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
1c. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
1d. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
2a. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	None
2b. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	none
3a. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U21, U22, U26, U117

Logical Interface Category	Logical Interfaces
3b. Interface between back office systems not under common management authority, for example: • Between a third party billing system and a utility meter data management system	U1
6. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U4, U20
7. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	None
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None
9. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
10a. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U6, U25, U32, U130
10b. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs, for example: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U42, U43, U44, U45, U49, U62, U124, U126, U127

Logical Interface Category	Logical Interfaces
12. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U18, U19, U42, U125
13. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U14, U29, U35
14. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U19, U24, U41, U46, U47, U48, U50, U128, U129
15. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
16. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	None
17. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
18. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	Not assessed in this draft

2.6 WIDE AREA SITUATIONAL AWARENESS (WASA)

Wide-area situational awareness (WASA) includes the monitoring and display of power-system components and performance across interconnections and over large geographic areas in near real-time. The goals of situational awareness are to understand and ultimately optimize the management of power-network components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions can arise.

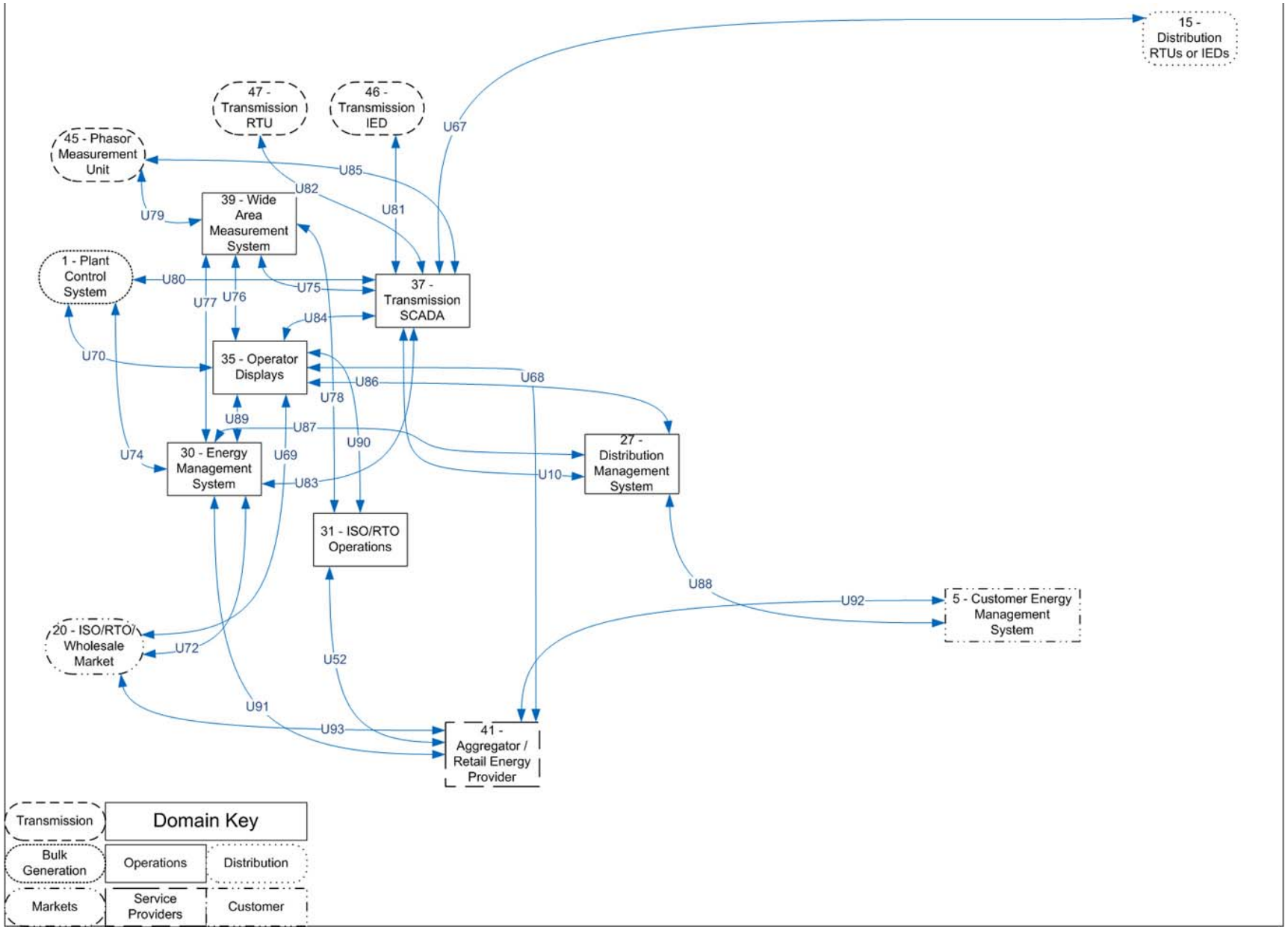

Figure 2.7 Wide Area Situational Awareness (WASA)

Table 2.7 – WASA Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1a. 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	U67, U79, U81, U82, U85
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
1c. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
1d. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
2a. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	None
2b. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U10, U70, U74, U80, U83, U84, U86, U87, U89, U90
3a. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	None

Logical Interface Category	Logical Interfaces
3b. Interface between back office systems not under common management authority, for example: • Between a third party billing system and a utility meter data management system	None
6. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U69, U72, U93
7. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U52, U68, U75, U91
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None
9. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
10a. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	None
10b. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs, for example: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	None

Logical Interface Category	Logical Interfaces
12. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U88, U92
13. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
14. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	None
15. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	U76, U77, U78
16. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	None
17. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
18. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

CHAPTER THREE
HIGH LEVEL SECURITY REQUIREMENTS

Some of the security requirements for the information infrastructure of the Smart Grid are similar to corporate information security requirements. For example, the security requirements of back office and corporate systems can be identified through assessments similar to those described in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. There are some differences, specifically, power system operations of the Smart Grid are more closely aligned with Industrial Control Systems as described in NIST Special Publication (SP) 800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*. With the implementation of the Smart Grid, IT and electric sector systems will be more closely associated. For example, customer interactions with utilities and third parties may include mixtures of power system operational information with high reliability and availability requirements and sensitive personal information with high confidentiality requirements.

This chapter includes the source documents and analysis results that were used to select the security requirements for the logical interface categories. The analysis was performed in the following steps:

1. Additional description of the logical interface categories. Identification and allocation of attributes to the logical interface categories (Table 3.1)
2. Determination of the confidentiality, integrity, and availability impact levels for each of the logical interface categories (Table 3.3). The focus is on power system reliability.
3. Initial selection of the security requirements applicable to the Smart Grid (Table 3.4). The common governance, risk and compliance (GRC) and common technical requirements are identified.
4. The unique technical requirements (excluding the GRC and common technical requirements) are allocated to the logical interface categories (Table 3.5).

This information is provided to organizations that are implementing, designing, and/or operating Smart Grid systems as a starting point for selecting and tailoring security requirements. Each organization will need to perform a risk analysis to determine the applicability of the following material.

3.1 CYBER SECURITY OBJECTIVES

In general for IT systems, the priority for the security objectives is confidentiality first, then integrity and availability. For industrial control systems, including power systems, the priorities of the security objectives are availability first, integrity second, and then confidentiality.

Availability is the most important security objective. The time latency associated with availability can vary:

- 4 ms for protective relaying;
- Sub-seconds for transmission wide-area situational awareness monitoring;

- Seconds for substation and feeder supervisory control and data acquisition (SCADA) data;
- Minutes for monitoring non-critical equipment and some market pricing information;
- Hours for meter reading and longer term market pricing information; and
- Days/weeks/months for collecting long term data such as power quality information.

Integrity for power system operations includes assurance that:

- Data has not been modified without authorization;
- Source of data is authenticated;
- Timestamp associated with the data is known and authenticated; and
- Quality of data is known and authenticated.

Confidentiality is the least critical for power system reliability. However, confidentiality is becoming more important, particularly with the increasing availability of customer information online:

- Privacy of customer information;
- Electric market information; and
- General corporate information, such as payroll, internal strategic planning, etc.

3.2 Logical Interface Categories

As stated in Chapter Two, each logical interface in the unified diagram was allocated to a logical interface category. This was done because many of the individual logical interfaces are similar in their security-related characteristics, and can therefore be categorized together as a means to simplify the identification of the appropriate security requirements. These security-related logical interface categories were defined based on attributes that could affect the security requirements.

These logical interface categories and the associated attributes can be used as guidelines by organizations that are developing a cyber security strategy and implementing a risk assessment to select the security requirements. This information may also be used by vendors and integrators as they design, develop, implement, and maintain the security controls. The numbering of the logical interface categories is not significant, and will be renumbered in the next version of the NISTIR.

3.2.1 Logical Interface Categories 1a, 1b, 1c, and 1d

The logical interfaces categories 1a, 1b, 1c, and 1d cover communications between control systems (typically centralized applications such as a SCADA master station) and equipment as well as communications between equipment. The equipment is categorized with either high availability or not. The interface communication channel is categorized with either compute and/or bandwidth constraints or not. When determining the applicability of controls for these interfaces, several were deemed NA as they pertain to Human-to-Machine interaction. All activities involved with interfaces 1a, 1b, 1c, and 1d are typically Machine-to-Machine.

Furthermore, communication modes and types are similar between logical interface categories 1a, 1b, 1c, and 1d and can be defined as follows:

- Interface Data Communication Mode
    - Near Real-Time Frequency Monitoring Mode (milliseconds, sub-cycle based on a 60Hz system) (may or may not include control action communication)
    - High Frequency Monitoring Mode (2sec - 59sec scan rates)
    - Low Frequency Monitoring Mode (scan/update rates in excess of 1min, file transfers)
- Interface Data Communication Type
    - Monitoring and Control Data for real time control system environment (typical measurement and control points)
    - Equipment Maintenance and Analysis (numerous measurements on field equipment that is typically used for preventive maintenance and post analysis)
    - Equipment Management Channel (remote maintenance of equipment)

The characteristics which vary between and distinguish each are the availability requirements for the interface and the compute/communications constraints for the interface as follows:

- Availability Requirements - Availability requirements will vary between these interfaces and are driven primarily by the power system application which the interface supports and not by the interface itself. For example, a SCADA interface to a substation or pole-top RTU may have a HIGH availability requirement in one case due to it supporting critical monitoring and switching functions or a MODERATE to LOW availability if supporting an asset monitoring application.
- Communications and Compute Constraints - Compute constraints are associated with crypto requirements on the interface. The use of crypto typically has high CPU needs for mathematical calculations. Existing application type devices like RTUs, substation IEDs, meters, and others are typically not equipped with sufficient digital hardware to perform crypto or other security functions.

  Bandwidth constraints are associated with data volume on the interface. In this case, media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are feasible.

With these requirements and constraints, logical interface categories 1a, 1b, 1c, and 1d can be defined as follows:

1a. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints

- Between transmission SCADA in support of state estimation and substation equipment for monitoring and control data using a high frequency mode
- Between distribution SCADA in support of three phase real-time power flow and substation equipment for monitoring data using a high and low frequency mode

- Between transmission SCADA in support of AGC and DCS within a power plant for monitoring and control data using a high frequency mode
- Between SCADA in support of Volt/VAR control and substation equipment for monitoring and control data using a high and low frequency mode
- Between transmission SCADA in support of contingency analysis and substation equipment for monitoring data using high frequency mode

1b. Interface between control systems and equipment without high availability, and with compute and/or bandwidth constraints

- Between field devices and control systems for analyzing power system faults using a low frequency mode
- Between a control system historian and field devices for capturing power equipment attributes using a high or low frequency mode
- Between distribution SCADA and lower priority pole-top devices for monitoring field devices using a low frequency mode
- Between pole-top IEDs and other pole-top IEDs (not used of protection or automated switching) for monitoring and control in a high or low frequency mode

1c. Interface between control systems and equipment with high availability, without compute and/or bandwidth constraints

- Between transmission SCADA and substation automation systems for monitoring and control data using a high frequency mode
- Between EMS and generation control (DCS) and RTUs for monitoring and control data using a high frequency mode
- Between distribution SCADA and substation automation systems, substation RTUs, and pole-top devices for monitoring and control data using a high frequency mode
- Between a PMU device and a Phasor Data Concentrator (PDC) for monitoring data using a high frequency mode
- Between IEDs (peer-to-peer) for power system protection

1d. Interface between control systems and equipment without high availability, without compute and/or bandwidth constraints

- Between field device and asset monitoring system for monitoring data using a low frequency mode
- Between field devices (relays, DFRs, PQ) and event analysis systems for event, disturbance, and power quality data
- Between distribution SCADA and lower priority pole-top equipment for monitoring and control data in a high or low frequency mode

- Between pole-top IEDs and other pole-top IEDs (not used for protection or automated switching) for monitoring and control in a high or low frequency mode
- Between distribution SCADA and backbone network-connected collector nodes for lower priority distribution pole-top IEDs for monitoring and control in a high or low frequency mode

3.2.2 Logical Interface Category 2a

Interface Category 2a covers the interfaces between control systems within the same organization, for example:

- Between multiple DMS systems belonging to the same utility and
- Between subsystems within DCS and ancillary control systems within a power plant

Control systems with interfaces between them have the following characteristics and issues:

- Since control systems generally have high data accuracy and high availability requirements, the interfaces between them need to implement those security requirements even if they do not have the same requirements.
- The interfaces generally use communication channels (WANs and/or LANs) that are designed for control systems.
- The control systems themselves are usually in secure environments, such as within a utility control center or within a power plant.

3.2.3 Logical Interface Category 2b

Interface Category 2b covers the interfaces between control systems in different organizations, for example:

- Between an RTO/ISO EMS and a utility energy management system
- Between a Generation and Transmission (G&T) SCADA and a distribution CO-OP SCADA
- Between a transmission EMS and a distribution DMS in different utilities
- Between an EMS/SCADA and a power plant DCS

Control systems with interfaces between them have the following characteristics and issues:

- Since control systems generally have high data accuracy and high availability requirements, the interfaces between them need to implement those security requirements even if they do not have the same requirements.
- The interfaces generally use communication channels (WANs and/or LANs) that are designed for control systems.
- The control systems are usually in secure environments, such as within a utility control center or within a power plant.

- However, since the control systems are in different organizations, the establishment and maintenance of the chain of trust is more important.

3.2.4 Logical Interface Category 3a and 3b

Interface Category 3a covers the interfaces between back office systems which are under common management authority, e.g., between a Customer Information System and a Meter Data Management System. These interfaces are focused on confidentiality and privacy rather than on power system reliability.

Interface Category 3b covers the interfaces between back office systems which are not under common management authority, e.g., between a third party billing system and a utility meter data management system. These interfaces are focused on confidentiality and privacy rather than on power system reliability.

3.2.5 Logical Interface Category 4

{Deliberately removed}

3.2.6 Logical Interface Category 5

{Deliberately removed}

3.2.7 Logical Interface Category 6

Logical Interface Category 6 covers the interface with Business-to-Business (B2B) connections between systems usually involving financial or market transactions, for example:

- Between a Retail Aggregator and an Energy Clearinghouse

These B2B interactions have the following characteristics and issues:

- Confidentiality is important since the interactions involve financial transactions with potentially large financial impacts, and where confidential bids are vital to a legally operating market.
- Privacy, in terms of historical information on what energy and/or ancillary services were bid, is important to maintain legal market operations, and avoiding market manipulation or gaming.
- Timing latency (critical time availability) and integrity are also important, although in a different manner than for control systems. For financial transactions involving bidding into a market, timing can be crucial. Therefore, although average availability does not need to be high, time latency during critical bidding times is crucial to avoid either inadvertent missed opportunities or deliberate market manipulation or gaming of the system.
- By definition, market operations are across organizational boundaries, thus posing trust issues.
- It is expected that many customers, possibly through aggregators or other energy service providers, will participate in the retail energy market, thus vastly increasing the number of participants.

- Special communication networks are not expected to be needed for the market transactions, and may include the public Internet as well as other available wide area networks.
- Although the energy market has now been operating for over a decade at the bulk power level, the retail energy market is in its infancy. Its growth over the next few years is expected, but no one yet knows in what directions or to what extent.
- However, systems and procedures for market interactions are a very mature industry. The primary requirement therefore is to utilize those concepts and protections in the newly emerging retail energy market.

3.2.8 Logical Interface Category 7

Logical Interface Category 7 covers the interfaces between control systems and non-control/corporate systems, for example:

- Between a Work Management System and a Geographic Information System
- Between a Distribution Management System and a Customer Information System
- Between an Outage Management System and the AMI Headend
- Between an Outage Management System and a Work Management System

These interactions between control systems and non-control systems have the following characteristics and issues:

- The primary security issue is preventing unauthorized access to sensitive control systems through non-control systems. As a result, integrity is the most critical security requirement.
- Since control systems generally require high availability, any interfaces with non-control systems should ensure that interactions with these other systems do not compromise the high reliability requirement.
- The interactions between these systems usually involve loosely-coupled interactions with very different types of exchanges from one system to the next and from one vendor to the next. Therefore standardization of these interfaces is still a work-in-progress, with the IEC 61970/69 Common Information Model (CIM) and NRECA's MultiSpeak expected to become the most common standards although other efforts for special interfaces (e.g. GIS) are also underway.

3.2.9 Logical Interface Category 8

Logical Interface Category 8 addresses the interfaces between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, e.g., between a temperature sensor on a transformer and its receiver. These sensors are very limited in compute capability and often in communication bandwidth.

3.2.10 Logical Interface Category 9

Logical Interface Category 9 addresses interfaces between sensor networks and control systems, e.g. between a sensor receiver and the substation master. These sensor receivers are usually limited in capabilities other than collecting sensor information.

3.2.11 Logical Interface Category 10a

Logical Interface Category 10a covers the interfaces between systems that use the AMI network, for example:

- Between MDMS and meters
- Between LMS/DRMS and Customer EMS

The issues for this Interface Category include the following:

- Most information from the customer must be treated as confidential.
- Integrity of data is clearly important in general, but alternate means for retrieving and/or validating it can be used.
- Availability is generally low across AMI networks since they are not designed for real-time interactions or rapid request-response requirements.
- Volume of traffic across AMI networks must be kept low to avoid denial of service situations.
- Meters are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied.
- Revenue-grade meters must be certified, so that patches and upgrades require extensive testing and validation.
- Meshed wireless communication networks are often used, which can present challenges related to wireless availability as well as throughput and configurations.
- Key management of millions of meters and other equipment will pose significant challenges that have not yet been addressed as standards.
- Remote disconnect could cause unauthorized outages.
- Due to the relatively new technologies used in AMI networks, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing.
- AMI networks span across organizations between utilities with corporate security requirements and customers with no or limited security capabilities or understandings.
- Utility-owned meters are in physically insecure locations that are not under utility control, limiting physical security.
- Many possible future interactions across the AMI network are still being designed, are just being speculated about, or have not yet been conceived.
- Customer reactions to AMI systems and capabilities are as yet unknown, and some may fear or reject the intrusion of such “Big Brother” systems.

3.2.12 Logical Interface Category 10b

Logical Interface Category 10b covers the interfaces between systems that use the AMI network with high availability, for example:

- Between LMS/DRMS and Customer DER
- Between DMS Applications and Customer DER
- Between DMS Applications and DA Field Equipment

Although both Interface Categories 10a and 10b use the AMI network to connect to field sites, the issues for this Interface Category 10b differ from those of 10a because the interactions are focused on power operations of Distributed Energy Resources (DER) and Distribution Automation (DA) equipment. Therefore the issues include the following:

- Although some information from the customer should be treated as confidential, most of the power system operational information does not need to be confidential.
- Integrity of data is very important since it can affect the reliability and/or efficiency of the power system.
- Availability will need to be a higher requirement for those parts of the AMI networks that will be used for real-time interactions and/or rapid request-response requirements.
- Volume of traffic across AMI networks will still need to be kept low to avoid denial of service situations.
- Meshed wireless communication networks are often used, which can present challenges related to wireless availability as well as throughput and configurations.
- Key management of large numbers of DER and DA equipment will pose significant challenges that have not yet been addressed as standards.
- Remote disconnect could cause unauthorized outages.
- Due to the relatively new technologies used in AMI networks, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing. This is particularly true for protocols used for DER and DA interactions.
- AMI networks span across organizations between utilities with corporate security requirements and customers with no or limited security capabilities or understandings. Therefore, maintaining the level of security needed for DER interactions will be challenging.
- DER equipment, and to some degree DA equipment, are in physically insecure locations that are not under utility control, limiting physical security.
- Many possible future interactions across the AMI network are still being designed, are just being speculated about, or have not yet been conceived. These could impact the security of the interactions with DER and DA equipment.

3.2.13 Logical Interface Category 11

Logical Interface Category 11 covers the interface between systems that use customer (residential, commercial, and industrial) site networks such as Home Area Networks (HANs), Building Area Networks (BANs), and Neighborhood Area Networks (NANs), for example:

- Between Customer EMS and Customer Appliances
- Between Customer EMS and Customer DER equipment
- Between Energy Service Interface and PEVs

The security-related issues for this intra-customer-site HAN/BAN/NAN Interface Category include the following:

- Some information exchanged among different appliances and systems must be treated as confidential to ensure that an unauthorized third party does not gain access to it. For instance, energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential from other appliances whose vendors may want to scavenge this information for marketing purposes.
- Integrity of data is clearly important in general, but since so many different types of interactions are taking place, the integrity requirements will need to be specific to the particular application.
- Availability is generally low across HAN networks since most interactions are not needed in real-time. Even DER generation and storage devices have their own integrated controllers which are normally expected to run independently of any direct monitoring and control, and must have "default" modes of operation to avoid any power system problems.
- Bandwidth is not generally a concern, since most HAN network media will be local wireless (e.g., WiFi, ZigBee, Bluetooth) or power line (e.g., HomePlug). The latter may be somewhat bandwidth limited, but can always be replaced by cable or wireless if the bandwidth is needed.
- Some HAN devices are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied.
- Wireless communication networks are expected to be used within the HAN, which could present some challenges related to wireless configuration and security, because most HANs will not have security experts managing these systems. For instance, if available security measures are not properly set, the HAN security could be compromised by any one of the internal devices as well as by external entities searching for these insecure HANs.
- Key management of millions of devices within millions of HANs will pose significant challenges that have not yet been addressed as standards.
- Due to the relatively new technologies used in HAN networks, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing. For instance, the Smart Energy Profile (SEP v2) is not expected to be widely available or stable for at least a couple of years.

- HAN networks will be accessible by many different vendors and organizations with unknown corporate security requirements and equally variable degrees and types of security solutions. Even if one particular interaction is "secure", in aggregate the multiplicity of interactions may not be secure.
- Some HAN devices may be in physically insecure locations, thus limiting physical security. Even those presumably "physically secure" within a home are vulnerable to inadvertent situations such as poor maintenance and misuse, as well as break-ins and theft.
- Many possible future interactions within the HAN environment are still being designed, are just being speculated about, or have not yet been conceived.

3.2.14 Logical Interface Category 12

Logical Interface Category 12 covers the Interface between external systems and the customer site, for example:

- Between Third Party and HAN Gateway
- Between ESP and DER
- Between Customer and CIS Web site

The security-related issues for this external interface to the customer site include the following:

- Some information exchanged among different appliances and systems must be treated as confidential and private to ensure that an unauthorized third party does not gain access to it. For instance, energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential from other appliances whose vendors may want to scavenge this information for marketing purposes.
- Integrity of data is clearly important in general, but since so many different types of interactions are taking place, the integrity requirements will need to be specific to the particular application.
- Availability is generally not critical between external parties and the customer site since most interactions are not related to power system operations nor are they needed in real-time. Even DER generation and storage devices have their own integrated controllers which are normally expected to run independently of any direct monitoring and control, and should have "default" modes of operation to avoid any power system problems.
- Bandwidth is not generally a concern, since higher speed media can be used if a function requires higher volume of data traffic. Many different types of media, particularly public media, is increasingly available, including the public Internet over cable or DSL, campus or corporate Intranets, cell phone GPRS, and neighborhood WiMAX and WiFi systems.
- Some customer devices that contain their own "HAN gateway" firewall are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied with those devices.
- Other than those used over the public Internet, communication protocols between third parties and ESI/HAN Gateways have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing.

- ESI/HAN Gateways will be accessible by many different vendors and organizations with unknown corporate security requirements and equally variable degrees and types of security solutions. Even if one particular interaction is "secure", in aggregate the multiplicity of interactions may not be secure.
- ESI/HAN Gateways may be in physically insecure locations, thus limiting physical security. Even those presumably "physically secure" within a home are vulnerable to inadvertent situations such as poor maintenance and misuse, as well as break-ins and theft.
- Many possible future interactions within the HAN environment are still being designed, are just being speculated about, or have not yet been conceived, leading to many possible but unknown security issues.

3.2.15 Logical Interface Category 13

Logical Interface Category 13 covers the interfaces between systems and mobile field crew laptops/equipment, for example:

- Between field crews and a Geographic Information System (GIS)
- Between field crews and CIS
- Between field crews and substation equipment
- Between field crews and OMS
- Between field crews and WMS
- Between field crews and AMI systems
- Between field crews and corporate marketing systems

As with all other logical interface categories, only the interface security requirements are addressed, not the inherent vulnerabilities of the end equipment such as the laptop or PDA used by the field crew.

The main activities performed on this interface include:

- Retrieving maps and/or equipment location information from GIS
- Retrieving customer information from CIS
- Providing equipment and customer updates, such as meter, payment and customer information updates to CIS
- Obtaining and providing substation equipment information, such as location, fault, testing, and maintenance updates
- Obtaining outage information and providing restoration information, including equipment, materials and resource information from/to OMS
- Obtaining project and equipment information and providing project, equipment, materials, resource, and location updates from/to WMS
- Obtaining metering and outage/restoration verification information from AMI systems
- Obtaining customer and product information for upsell opportunities

The key characteristics of interface category 13 include:

- This interface is primarily for customer service operations. The most critical needs for this interface are:
  - To post restoration information back to the OMS for reprediction of further outage situations
  - To receive reconnection information for customers who have been disconnected
- Information exchanged between these systems is typically corporate owned and security is managed within the utility between the interfacing applications. Increased use of wireless technologies and external service providers adds a layer of complexity in security requirements that is addressed in all areas where multi-vendor services are interfaced with utility systems.
- Most metering information obtained from the customer by field devices must be treated as confidential since profiles of hourly energy usage (as opposed to monthly energy usage) could be used for unauthorized and/or illegal activities.
- Integrity of data is clearly important in general, but since so many different types of interactions are taking place, the integrity requirements will need to be specific to the particular application. However, the integrity of revenue-grade metering data that may be collected in this manner is vital since it has a direct financial impact on all stakeholders of the loads and generation being metered.
- Availability is generally not very critical as interactions are not necessary for real time. Exceptions include payment information for disconnects, restoration operations, and efficiency of resource management.
- Bandwidth is not generally a concern as most utilities have sized their communications infrastructure to meet the needs of the field applications and most field applications have been designed for minimal transmission of data in wireless mode. However, more and more applications are being given to field crews to enhance customer service opportunities and for tracking and reporting of construction, maintenance and outage restoration efforts. This will increase the amount of data and interaction between the corporate systems, third party providers and the field crews.
- Data held on laptops and PDAs is vulnerable to physical theft due to the inherent nature of mobile equipment, but those physical security issues will not be addressed in this section. In addition, most mobile field applications are designed to transmit data as it is input and therefore data is not when the volume of data is too large to transmit over wireless and some areas do not have wireless coverage. In both cases, data is maintained on the laptop/PDA until reconnected to a physical network.

3.2.16 Logical Interface Category 14

Logical Interface Category 14 covers the interface between metering equipment, for example:

- Between sub-meter to meter
- Between PEV meter and Energy Service Provider

- Between MDMS and meters (via the AMI headend)
- Between customer EMS and meters
- Between field crew tools and meters
- Between customer DER and sub-meters
- Between electric vehicles and sub-meters

The issues for this Metering Interface Category include the following:

- Most metering information from the customer must be treated as confidential since profiles of hourly energy usage (as opposed to monthly energy usage) could be used for unauthorized and/or illegal activities.
- Integrity of revenue-grade metering data is vital since it has a direct financial impact on all stakeholders of the loads and generation being metered.
- Availability of metering data is important but not critical, since alternate means for retrieving metering data can still be used.
- Meters are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied.
- Revenue-grade meters must be certified, so that patches and upgrades require extensive testing and validation.
- Key management of millions of meters will pose significant challenges that have not yet been addressed as standards.
- Due to the relatively new technologies used with smart meters, some standards have not been fully developed, nor have their capabilities been proven through rigorous testing.
- Multiple (authorized) stakeholders, including customers, utilities, and third parties, may need access to energy usage either directly from the meter or after it has been processed and validated for settlements and billing, thus adding cross-organizational security concerns.
- Utility-owned meters are in physically insecure locations that are not under utility control, limiting physical security.
- Customer reactions to AMI systems and smart meters are as yet unknown, and some may fear or reject the intrusion of such “Big Brother” systems.

3.2.17 Logical Interface Category 15

Logical Interface Category 15 covers the interfaces between operations decision support systems, e.g. between Wide Area Measurement Systems (WAMS) and ISO/RTOs. Due to the very large coverage of these interfaces, the interfaces are more sensitive to confidentiality requirements than other operational interfaces (see logical interface category 1).

3.2.18 Logical Interface Category 16

Logical Interface Category 16 covers the interfaces between engineering/maintenance systems

and control equipment, for example:

- Between engineering and substation relaying equipment for relay settings
- Between engineering and pole-top equipment for maintenance
- Within power plants

The main activities performed on this interface include:

- Installing and changing device settings. These may include operational settings (such as relay settings, thresholds for unsolicited reporting, thresholds for device mode change, and editing of setting groups), event criteria for log record generation, and criteria for oscillography recording.
- Retrieving maintenance information
- Retrieving device event logs
- Retrieving device oscillography files
- Software updates
- Possibly, security settings and audit log retrieval (if the security audit log is separate from the event logs)

The key characteristics of logical interface category 16 include:

- The functions performed on this interface are not considered real-time.
- Some communications carried on this interface may be performed interactively.
- The principal driver for urgency on this interface is the need for information to analyze a disturbance.
- Although the present impact level for this interface indicates low confidentiality, this should be raised to at least medium.
- Device settings should be treated as critical infrastructure information, requiring confidentiality.
- Logs and files containing forensic evidence following events should likely remain confidential for both critical infrastructure and organizational reasons, at least until analysis has been completed.
- These functions are presently performed by a combination of:
  - Separate remote access to devices, such as by dial-up
  - Local access at the device (addressed in logical interface category 13)
  - Access via the same interface used for real-time communications

3.2.19 Logical Interface Category 17

Logical Interface Category 17 covers the interfaces between control systems and their vendors for standard maintenance and service:

- Between SCADA system and its vendor

Note: In the architecture diagram, the vendor actor is currently embedded in the distribution engineering or (not yet appearing) transmission engineering actor. It will be separated in a later version of the NISTIR.

The main activities performed on this interface include:

- Firmware and/or software updates
- Retrieving maintenance information
- Retrieving event logs

Key characteristics of logical interface category 17 include:

- The functions performed on this interface are not considered real-time.
- Some communications carried on this interface may be performed interactively.
- The principal driver for urgency on this interface is the need for critical operational/security updates.
- These functions are presently performed by a combination of:
  - Separate remote access to devices, such as by dial-up
  - Local access at the device/control system console
  - Access via the same interface used for real-time communications

Activities outside of the scope of Logical Interface Category 17 include:

- Vendors acting in an (outsourced) operational role (see logical interface categories 1, 2 or 16, depending upon the role)

3.2.20 Logical Interface Category 18

Logical Interface category 18 covers the interfaces between security/network/system management consoles and all networks and systems:

- Between a security console and network routers, firewalls, computer systems, and network nodes

The main activities performed on this interface include:

- Communication infrastructure operations and maintenance
- Security infrastructure operations and maintenance

Key characteristics of logical interface category 18 include:

- The functions performed on this interface are not considered real-time.
- Some communications carried on this interface may be performed interactively.
- The principal driver for urgency on this interface is the need for critical operational/security updates.

- These functions are presently performed by a combination of:
  - Separate remote access to devices, such as by dial-up
  - Local access at the device/control system console
  - Access via the same interface used for real-time communications

Activities outside of the scope of logical interface category 18 include:

- Smart Grid transmission and distribution (see logical interface categories 1 and 2)
- Advanced metering (see logical interface category 10)
- Control systems engineering and systems maintenance (see logical interface category 16)

3.2.21 Analysis Matrix of Interface Categories

A set of Smart Grid key attributes was defined and allocated to each logical interface category. These key attributes included requirements and constraints that were used in the selection of security requirements for the logical interface category. Table 3.1 provides the analysis matrix of the security-related logical interface categories (rows) against the attributes that reflect the interface categories (columns).This analysis was one of the tools that was used in the determination of the confidentiality, integrity and availability impact levels for each logical interface category and in the selection of security requirements.

Table 3.1 Analysis Matrix of Security-Related Logical Interface Categories, Defined by Attributes (ATR)

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
1a. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints			X	X	X	X	X	X		X	X	X	X	X	X		X		X
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints			X		X	X	X	X		X	X	X	X	X	X		X	X	X
1c. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints			X	X			X	X		X	X	X	X	X	X		X		X

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
1d. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints			X				X	X		X	X	X	X	X	X	X	X		X
2a. Interface between control systems within the same organization			X	X						X		X			X				X
2b. Interface between control systems in different organizations			X	X					X	X		X			X				
3a. Interface between back office systems under common management authority	X	X	X												X				

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
3b. Interface between back office systems not under common management authority	X	X	X						X						X				
6. Interface with B2B connections between systems usually involving financial or market transactions	X	X	X	X					X	X						X			
7. Interface between control systems and non-control/ corporate systems	X	X	X	X				X	X						X	X			
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements					X	X	X	X		X	X	X	X				X	X	

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
9. Interface between sensor networks and control systems			X		X	X	X	X		X	X	X		X			X	X	X
10a. Interface between systems that use the AMI network	X	X	X		X	X	X	X	X				X	X	X	X	X		
10b. Interface between systems that use the AMI network for functions that require high availability	X	X	X	X	X	X	X	X	X				X	X	X	X	X		
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs	X	X	X	X		X	X	X	X	X			X	X		X	X		X
12. Interface between external systems and the customer site	X	X	X			X		X	X				X	X		X			

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
13. Interface between systems and mobile field crew laptops/equipment	X		X	X	X		X	X					X	X	X		X		
14. Interface between metering equipment	X	X	X		X	X	X	X	X		X	X	X	X	X		X		
15. Interface between operations decision support systems			X	X					X	X									
16. Interface between engineering/ maintenance systems and control equipment			X		X	X					X	X	X	X	X		X		
17. Interface between control systems and their vendors for standard maintenance and service			X						X				X	X	X		X		

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
18. Interface between security/network/ system management consoles and all networks and systems	X	X	X	X						X	X	X		X	X	X	X		

3.3 CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (C, I, AND A) IMPACT LEVELS

Following are the definitions for the security objectives of confidentiality, integrity and availability, as defined in statute.

Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of *integrity* is the unauthorized modification or destruction of information.

Availability

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

Based on these definitions, impact levels for each security objective (confidentiality, integrity, and availability) are specified as low, moderate, and high as defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. (see Table 3.2 below) The impact levels are used in the selection of security requirements for each logical interface category.

Table 3.2 Impact Levels Definitions

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations,

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
	assets, or individuals.	assets, or individuals.	organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

3.4 IMPACT LEVELS FOR THE CATEGORIES

Each of the three impact levels (i.e., low, moderate, high) is based upon the expected adverse effect of a security breach upon organizational operations, organizational assets, or individuals. The initial designation of impact levels focused on power grid reliability. The expected adverse effect on individuals when privacy breaches occur and adverse effects on

financial markets when confidentiality is lost are included in specific logical interface categories listed below.

- **Power system reliability**: Keep electricity flowing to customers, businesses, and industry. For decades, the power system industry has been developing extensive and sophisticated systems and equipment to avoid or shorten power system outages. In fact, power system operations have been termed the largest and most complex machine in the world. Although there are definitely new areas of cyber security concerns for power system reliability as technology opens new opportunities and challenges, nonetheless, the existing energy management systems and equipment, possibly enhanced and expanded, should remain as key cyber security solutions.
- **Confidentiality and privacy of customers**: As the Smart Grid reaches into homes and businesses, and as customers increasingly participate in managing their energy, confidentiality and privacy of their information has increasingly become a concern. Unlike power system reliability, customer privacy is a new issue.

The impact levels presented in Table 3.3 – Power System Reliability Impact Levels – focus on impacts to the nation-wide power grid, particularly with regard to grid stability and reliability. This is an initial analysis and will be revised over the next several months.

Table 3.3 Power System Reliability Impact Levels

Interface Category	Confidentiality	Integrity	Availability	Additional Issues
1a	L	H	H	
1b	L	H	M	
1c	L	H	H	
1d	L	H	M	
2b	L	H	M	
2a	L	H	H	
3a	H	M	L	Primarily addresses confidentiality and privacy
3b	H	M	L	Primarily addresses confidentiality and privacy
6*	L	M	M	
7	L	H	M	
8	L	M	M	
9	L	M	M	
10a	L	H	L	
10b	L	H	H	
11	L	M	M	For power system reliability, the

Interface Category	Confidentiality	Integrity	Availability	Additional Issues
				confidentiality level is low. If a logical interface within this category sends sensitive information, the confidentiality level will be high.
12*	H	M	L	Primarily addresses confidentiality and privacy
13	L	H	M	Critical security parameters (CSPs) need to be encrypted for confidentiality
14	L	H	L	For power system reliability, the confidentiality level is low. If a logical interface within this category sends sensitive information, the confidentiality level will be high.
15	L	H	M	
16	L	H	M	
17	L	H	L	
18	H	H	H	

Logical interface categories 3a, 3b and 12 do not primarily address power system reliability; they primarily address the confidentiality and privacy of information.

3.5 RECOMMENDED SECURITY REQUIREMENTS

Power system operations pose many security challenges that are different from most other industries. For example, the Internet is different from the power system operations environment. In particular, there are strict performance and reliability requirements that are needed by power system operations. For instance:

- Operation of the power system must continue 24x7 with high availability (e.g. 99.99% for SCADA and higher for protective relaying) regardless of any compromise in security or the implementation of security measures which hinder normal or emergency power system operations.
- Power system operations must be able to continue during any security attack or compromise (as much as possible).
- Power system operations must recover quickly after a security attack or compromised information system.
- Testing of security measures cannot be allowed to impact power system operations.

There is no single set of cyber security requirements that addresses each of the Smart Grid logical interface categories. This information can be used as guidelines for actual implementations.

The following table includes all the proposed requirements for the Smart Grid. The requirements were selected from NIST SP 800-53 and the DHS Catalog. This list may be expanded to add requirements from NIST SP 800-82, NIST SP 800-63, and the NERC CIPs, as applicable. Each requirement was allocated to Common Governance, Risk and Compliance (GRC); Common Technical; or Unique Technical categories. The intent of the GRC requirements is to have them developed at the organization level. It may be necessary to augment these organization level requirements for specific logical interface categories and/or systems. Also, several requirements are specific to the federal government – these have been specified. The remaining requirements are the technical requirements. There are several that are applicable to all the logical interface categories, and these have been identified as common technical requirements. The remaining technical requirements are allocated to one or more of the logical interface categories in table 3.4 below. These are the specific technical requirements that should be considered by an organization when implementing a Smart Grid system. In the next version of the NISTIR, all requirements and requirement enhancements will be further analyzed to determine if they should be tailored.

The requirements should be allocated to each Smart Grid system and not necessarily to every component within that specific system. The focus is on security at the system level.

For each requirement, the proposed baselines – low, moderate, high – are listed. The numbers in parentheses in the baselines are the control enhancements applicable for each baseline. The baselines were developed using SP 800-53 and augmented with the additional DHS Catalog requirements. The SP 800-53 baselines focus on the impact for IT systems, with the highest

priority for confidentiality. For the Smart Grid the priorities are availability and integrity. Therefore, the list of baselines is a starting point for the Smart Grid.

Table 3.4 – Proposed Requirements for the Smart Grid[21]

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.1.1	Security Policies and Procedures	X			L, M, H
2.2.1	Management Policies and Procedures	X			L, M, H
2.2.2	Management Accountability	X			L, M, H
2.2.3	Baseline Practices	X			L, M, H L, M, H
2.2.4	Coordination of Threat Mitigation	X			L, M, H
2.2.5	Security Policies for Third Parties	X			L, M, H
2.2.6	Termination of Third Party Access	X			L, M, H L, M, H
2.3.1	Personnel Security Policies and Procedures	X			L, M, H
2.3.2	Position Categorization	X			L, M, H
2.3.3	Personnel Screening	X			L, M, H
2.3.4	Personnel Termination	X			L, M, H
2.3.5	Personnel Transfer	X			L, M, H
2.3.6	Access Agreements	X			L, M, H
2.3.7	Third Party Personnel Security	X			L, M, H
2.3.8	Personnel Accountability	X			L, M, H
2.3.9	Personnel Roles	X			L, M, H
2.4.1	Physical and Environmental Security Policies and Procedures	X			L, M, H
2.4.2	Physical Access Authorizations	X			L, M, H
2.4.3	Physical Access Control	X			L, M, H (1)
2.4.4	Monitoring Physical	X			L, M (1), H

[21] The revised DHS Catalog is located at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628Feb2010/FINAL__Catalog_of_Recommendations_Rev_4_mod_01-18-10.doc

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
	Access				(1,2)
2.4.5	Visitor Control	X			L, M (1), H (1)
2.4.6	Visitor Records	X			L, M, H (1)
2.4.7	Physical Access Log Retention	X			L, M, H
2.4.8	Emergency Shutoff	X			M, H
2.4.9	Emergency Power	X			M, H (1)
2.4.10	Emergency Lighting	X			L, M, H
2.4.11	Fire Protection	X			L, M (1,2,3), H (1,2,3)
2.4.12	Temperature and Humidity Controls	X			L, M, H
2.4.13	Water Damage Protection	X			L, M, H (1)
2.4.14	Delivery and Removal	X			L, M, H
2.4.15	Alternate Work Site	X			M, H
2.4.16	Portable Media	X			L, M (1,2,3), H (1,2,3)
2.4.17	Personnel and Asset Tracking	X			L, M, H
2.4.18	Location of Control System Assets	X			M, H (1)
2.4.20	Power Equipment and Power Cabling	X			M, H
2.4.21	Physical Device Access Control	X			L, M, H
2.5.1	System and Services Acquisition Policy and Procedures	X			L, M, H
2.5.2	Allocation of Resources	X			L, M, H
2.5.3	Life-Cycle Support	X			L, M, H
2.5.4	Acquisitions	X			L, M (1), H (1,2)
2.5.5	Control System Documentation	X			L, M (1,3), H (1,2,3)
2.5.6	Software License Usage Restrictions	X			L, M, H
2.5.7	User-installed Software	X			L, M, H
2.5.8	Security Engineering Principals	X			M, H

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.5.9	Outsourced Control System Services	X			L, M, H
2.5.10	Vendor Configuration Management	X			M, H
2.5.11	Vendor Security Testing		X		M,H
2.5.12	Supply Chain Protection			X	H
2.5.13	Trustworthiness			X	H
2.6.1	Configuration Management Policy and Procedures	X			L, M, H
2.6.2	Baseline Configuration	X			L, M (1), H (1,2,5,6)
2.6.3	Configuration Change Control	X			M (2), H (1,2)
2.6.4	Monitoring Configuration Changes	X			L, M, H
2.6.5	Access Restrictions for Configuration Change	X			M, H (1,2,3)
2.6.6	Configuration Settings	X			L, M (3), H (1,2,3)
2.6.7	Configuration for Least Functionality		X		L, M, H
2.6.8	Configuration Assets		X		L, M, H
2.6.9	Addition, Removal, and Disposition of Equipment	X			L, M, H L, M, H
2.6.10	Factory Default Authentication Management	X			L, M, H
2.6.11	Configuration Management Plan	X			M, H
2.7.1	Strategic Planning Policy and Procedures	X			L, M, H
2.7.2	Control System Security Plan	X			L, M, H
2.7.3	Interruption Identification and Classification	X			L, M, H L, M, H
2.7.4	Incident Roles and Responsibilities	X			L, M, H L, M, H
2.7.5	Planning Process Training	X			L, M, H

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.7.6	Testing	X			L, M, H
2.7.7	Investigate and Analyze	X			L, M, H
2.7.8	Corrective Action	X			L, M, H
2.7.9	Risk Mitigation	X			L, M, H L, M, H L, M, H
2.7.10	System Security Plan Update	X			L, M, H
2.7.11	Rules of Behavior	X			L, M, H
2.7.12	Security-Related Activity Planning	X			M, H
2.8.1	System and Communication Protection Policy and Procedures	X			L, M, H
2.8.2	Management Port Partitioning			X	M, H
2.8.3	Security Function Isolation			X	L, M, H
2.8.4	Information Remnants			X	M, H
2.8.5	Denial-of-Service Protection			X	L, M, H
2.8.6	Resource Priority			X	none
2.8.7	Boundary Protection			X	L, M (1,2,3,4,5,10), H (1,2,3,4,5,6,10,11)
2.8.8	Communication Integrity			X	M (1), H (1)
2.8.9	Communication Confidentially			X	M (1), H (1)
2.8.10	Trusted Path			X	none
2.8.11	Cryptographic Key Establishment and Management			X	L, M, H (1)
2.8.12	Use of Validated Cryptography			X	L, M, H
2.8.13	Collaborative Computing			X	L, M, H
2.8.14	Transmission of Security Parameters			X	none

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.8.15	Public Key Infrastructure Certificates			X	M, H
2.8.16	Mobile Code			X	M, H
2.8.17	Voice-over-Internet Protocol			X	M, H
2.8.18	System Connections			X	L, M, H
2.8.19	Security Roles			X	L, M, H L, M, H
2.8.20	Message Authenticity			X	M, H
2.8.21	Architecture and Provisioning for Name/Address Resolution Service			X	M, H
2.8.22	Secure Name/Address Resolution Service (Authoritative Source)			X	L (1), M (1), H (1)
2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver)			X	H
2.8.24	Fail in Known State			X	H
2.8.25	Thin Nodes			X	None
2.8.26	Honeypots			X	None
2.8.27	Operating System-Independent Applications			X	None
2.8.28	Confidentiality of Information at Rest			X	M, H
2.8.29	Heterogeneity			X	none
2.8.30	Virtualization Techniques			X	None
2.8.31	Covert Channel Analysis			X	None
2.8.32	Application Partitioning			X	M, H
2.8.33	Information System Partitioning			X	M, H
2.9.1	Information and Document Management Policy and Procedures	X			L, M, H
2.9.2	Information and Document Retention	X			L, M, H
2.9.3	Information Handling	X			L, M, H

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.9.4	Information Classification	X			L, M, H
2.9.5	Information Exchange	X			
2.9.6	Information and Document Classification	X			L, M, H L, M, H L, M, H
2.9.7	Information and Document Retrieval	X			L, M, H
2.9.8	Information and Document Destruction	X			L, M, H
2.9.9	Information and Document Management Review	X			L, M, H
2.9.10	Automated Marking	X			H
2.9.11	Automated labeling	X			none
2.10.1	System Maintenance Policy and Procedures	X			L, M, H
2.10.2	Legacy System Upgrades	X			L, M, H
2.10.3	System Monitoring and Evaluation	X			L, M, H L, M, H L, M, H
2.10.4	Backup and Recovery	X			L, M, H L, M, H
2.10.5	Unplanned System Maintenance	X			L, M, H
2.10.6	Periodic System Maintenance	X			L, M (1), H (1,2)
2.10.7	Maintenance Tools	X			M (1,2), H (1,2,3)
2.10.8	Maintenance Personnel	X			L, M, H
2.10.9	Remote Maintenance	X			L, M (1,2), H (1,2,3)
2.10.10	Timely Maintenance	X			M, H
2.11.1	Security Awareness Training Policy and Procedures	X			L, M, H
2.11.2	Security Awareness	X			L, M, H
2.11.3	Security Training	X			L, M, H
2.11.4	Security Training Records	X			L, M, H
2.11.5	Contact with Security	X			none

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
	Groups and Associations				
2.11.6	Security Responsibility Training	X			L, M, H
2.12.1	Incident Response Policy and Procedures	X			L, M, H
2.12.2	Continuity of Operations Plan	X			L, M, H
2.12.3	Continuity of Operations Roles and Responsibilities	X			L, M, H
2.12.4	Incident Response Training	X			L, M, H
2.12.5	Continuity of Operations Plan Testing	X			L, M (1), H (1,2) M, H (1)
2.12.6	Continuity of Operations Plan Update	X			L, M, H
2.12.7	Incident Handling	X			L, M (1), H (1)
2.12.8	Incident Monitoring	X			L, M, H (1)
2.12.9	Incident Reporting	X			L, M (1), H (1)
2.12.10	Incident Response Assistance	X			L, M (1), H (1)
2.12.11	Incident Response Investigation and Analysis	X			L, M, H
2.12.12	Corrective Action	X			L, M, H L, M, H
2.12.13	Alternative Storage Sites	X			M (1,2), H (1,2,3)
2.12.14	Alternate Command/Control Methods	X			M (1,3), H (1,3) M (1,2), H (1,2,3,4)
2.12.15	Alternate Control Center	X			M (1,2,3,5), H (1,2,3,4,5) M (1,2), H (1,2,3,4)
2.12.16	Control System Backup	X			L, M (1), H (1,2,3)
2.12.17	Control System Recovery and Reconstitution	X			L, M (2,3), H (2,3,4)

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.12.18	Fail-Safe Response	X			H
2.13.1	Media Protection and Procedures	X			L, M, H
2.13.2	Media Access	X			L, M (1), H (1)
2.13.3	Media Classification	X			M, H
2.13.4	Media Labeling	X			M, H
2.13.5	Media Storage	X			M, H
2.13.6	Media Transport	X			M (2), H (2,3)
2.13.7	Media Sanitization and Storage	X			L, M, H (1,2)
2.14.1	System and Information Integrity Policy and Procedures	X			L, M, H
2.14.2	Flaw Remediation		X		L, M (2), H (1,2)
2.14.3	Malicious Code Protection	X			L, M (1,2,3), H (1,2,3)
2.14.4	System Monitoring Tools and Techniques	X			M (2,4,5,6), H 2,4,5,6)
2.14.5	Security Alerts and Advisories	X			L, M, H (1)
2.14.6	Security Functionality Verification	X			H
2.14.7	Software and Information Integrity			X	M (1), H (1,2)
2.14.8	Spam Protection			X	M, H (1)
2.14.9	Information Input Restrictions	X			M, H
2.14.10	Information Input Accuracy, Completeness, Validity and Authenticity			X	M, H
2.14.11	Error Handling			X	M, H
2.14.12	Information Output Handling and Retention	X			L, M, H
2.14.13	Predictable Failure Prevention	X			none
2.15.1	Access Control Policies and Procedures	X			L, M, H
2.15.2	Identification and	X			L, M, H

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
	Authentication Procedures and Policy				
2.15.3	Account Management	X			L, M (1,2,3,4), H (1,2,3,4)
2.15.4	Identifier Management	X			L, M, H
2.15.5	Authenticator Management	X			L, M (1,2), H (1,2)
2.15.6	Supervision and Review	X			L, M, H L, M, H (1)
2.15.7	Access Enforcement	X			L, M, H
2.15.8	Separation of Duties			X	M, H
2.15.9	Least Privilege			X	M, H
2.15.10	User Identification and Authentication			X	L (1), M (1,2,3), H (1,2,3,4)
2.15.11	Permitted Actions without Identification and Authentication			X	L, M (1), H (1)
2.15.12	Device Authentication and Identification			X	M, H
2.15.13	Authenticator Feedback			X	L, M, H
2.15.14	Cryptographic Module Authentication			X	L, M, H
2.15.15	Information Flow Enforcement			X	M, H
2.15.16	Passwords			X	L, M, H
2.15.17 *(fed gov't reqmt)*	System Use Notification			X	L, M, H
2.15.18	Concurrent Session Control			X	H
2.15.19 *(fed gov't reqmt)*	Previous Logon Notification			X	none
2.15.20 *(fed gov't reqmt)*	Unsuccessful Logon Notification			X	L, M, H
2.15.21	Session Lock			X	M, H
2.15.22	Remote Session Termination			X	M, H (1)

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.15.23	Remote Access Policy and Procedures			X	L, M, H
2.15.24	Remote Access			X	L, M (1,2,3,4,6,10, 11,12), H (1,2,3,4,5,6,10,11,12),
2.15.25	Access Control for Portable and Mobile Devices			X	L, M (1,2,3), H (1,2,3)
2.15.26	Wireless Access Restrictions			X	L, M (1), H (1,2)
2.15.27	Personally Owned Information			X	L, M, H
2.15.28	External Access Protections	X			L, M, H
2.15.29	Use of External Information Control Systems	X			L, M (1,2), H (1,2)
2.15.30	Publicly Accessible Content	X			L, M, H
2.16.1	Audit and Accountability Process and Procedures	X			L, M, H
2.16.2	Auditable Events			X	L, M (3,4), H (3,4)
2.16.3	Content of Audit Records			X	L, M (1), H (1,2)
2.16.4	Audit Storage Capacity			X	L, M, H
2.16.5	Response to Audit Processing Failures	X			L, M, H (1,2)
2.16.6	Audit Monitoring, Analysis, and Reporting	X			L, M, H (1)
2.16.7	Audit Reduction and Report Generation	X			M (1), H (1)
2.16.8	Time Stamps	X			L, M (1), H (1)
2.16.9	Protection of Audit Information	X			L, M, H
2.16.10	Audit Record Retention	X			L, M, H
2.16.11	Conduct and Frequency of Audits	X			L, M, H L, M, H

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.16.12	Auditor Qualification	X			
2.16.13	Audit Tools	X			
2.16.14	Security Policy Compliance	X			L, M, H L, M, H
2.16.15	Audit Generation			X	L, M, H (1)
2.16.16	Non-Repudiation			X	H
2.17.1	Monitoring and Reviewing Control System Security management Policy and Procedures	X			L, M, H
2.17.2	Continuous Improvement	X			
2.17.3	Monitoring of Security Policy	X			L, M (1), H (1)
2.17.4	Best Practices	X			
2.17.5 *(fed gov't reqmt)*	Security Accreditation	X			L, M, H
2.17.6 *(fed gov't reqmt)*	Security Certification	X			L, M (1), H (1)
2.18.1	Risk Assessment Policy and Procedures	X			L, M, H
2.18.2	Risk Management Plan	X			L, M, H
2.18.3 *(fed gov't reqmt)*	Certification, Accreditation, and Security Assessment Policies and Procedures	X			L, M, H
2.18.4	Security Assessments	X			L, M, H
2.18.5	Control System Connections			X	L, M, H
2.18.6 *(fed gov't reqmt)*	Plan of Action and Milestones	X			L, M, H
2.18.7	Continuous Monitoring	X			L, M, H
2.18.8	Security Categorization	X			L, M, H
2.18.9	Risk Assessment	X			L, M, H
2.18.10	Risk Assessment Update	X			L, M, H
2.18.11	Vulnerability Assessment and Awareness	X			L, M (1), H (1,2,3,4,6,8)

DHS Catalog Ref No. (augmented)	Requirement Name	Common Governance, Risk, and Compliance (GRC) Reqs	Common Tech Reqs	Unique Tech Reqs	Baseline (using SP 800-53 as the starting point)
2.18.12	Identify, Classify, Analyze, and Prioritize Potential Security Risks	X			L, M, H
2.19.1	Security Program Plan	X			L, M, H
2.19.2	Senior Security Officer	X			L, M, H
2.19.3 *(fed gov't reqmt)*	Security Resources	X			L, M, H
2.19.4 *(fed gov't reqmt)*	Plan of Action and Milestones Process	X			L, M, H
2.19.5 *(fed gov't reqmt)*	System Inventory	X			L, M, H
2.19.6 *(fed gov't reqmt)*	Security Measures of Performance	X			L, M, H
2.19.7	Enterprise Architecture	X			L, M, H
2.19.8 *(fed gov't reqmt)*	Critical Infrastructure Plan	X			L, M, H
2.19.9	Risk Management Strategy	X			L, M, H
2.19.10 *(fed gov't reqmt)*	Security Authorization Process	X			L, M, H
2.19.11	Mission/Business Process Definition	X			L, M, H

3.6 TECHNICAL REQUIREMENTS ALLOCATED TO LOGICAL INTERFACE CATEGORIES

Table 3.5 lists the remaining technical requirements after the common governance, risk and compliance (GRC) requirements and the common technical requirements were extracted from the full list of requirements. These common technical requirements are implemented at the organization level, with augmentation, as required, for specific systems. The remaining technical requirements are allocated to logical interface categories, as applicable.

Table 3.5 – Allocation of Technical Requirements to the Logical Interface Categories

DHS Catalog Req	Logical Interface Categories																					
	1a	1b	1c	1d	2a	2b	3a	3b	6	7	8	9	10a	10b	11	12	13	14	15	16	17	18
2.8.2	X	X	X	X													X				X	X
2.8.3	X	X	X	X			X	X					X	X	X	X		X		X	X	X
2.8.4																						
2.8.5	X	X	X	X	X	X	X	X	X	X		X		X	X	X		X	X			X
2.8.6					X	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X
2.8.7	X	X	X	X	X	X		X	X	X		X	X	X	X	X		X	X	X	X	X
2.8.8	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X
2.8.9	X	X	X	X					X				X	X	X	X		X	X	X	X	X
2.8.10																						
2.8.11	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X
2.8.12	X	X	X	X		X	X	X					X	X	X	X		X	X	X	X	X
2.8.13	X	X	X	X																		
2.8.14	X	X	X	X	X	X			X	X			X	X	X	X		X				
2.8.15									X	X		X								X	X	X
2.8.16							X	X														
2.8.17																						
2.8.18					X	X	X	X	X					X	X	X		X	X	X	X	X
2.8.19					X	X	X	X	X	X			X	X	X	X		X	X	X	X	X

DHS Catalog Req	Logical Interface Categories																					
	1a	1b	1c	1d	2a	2b	3a	3b	6	7	8	9	10a	10b	11	12	13	14	15	16	17	18
2.8.20	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
2.8.21*	X	X	X	X																		X
2.8.22																						X
2.8.23																						X
2.8.24	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X
2.8.25																						
2.8.26																						
2.8.27																						
2.8.28							X	X		X			X	X	X	X		X				
2.8.29																						
2.8.30																						
2.8.31																						
2.8.32																						X
2.8.33																						X
2.14.7	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
2.14.8							X	X									X					
2.14.10	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	
2.14.11	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	
2.15.8	X	X	X	X			X	X											X			
2.15.9	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X		
2.15.10	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X		X	X	X
2.15.11	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X			X	X
2.15.12	X	X	X	X			X	X				X					X		X	X	X	X
2.15.13	X	X	X	X								X							X	X	X	X

DHS Catalog Req	Logical Interface Categories																					
	1a	**1b**	**1c**	**1d**	**2a**	**2b**	**3a**	**3b**	**6**	**7**	**8**	**9**	**10a**	**10b**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
2.15.14	X	X	X	X			X	X	X	X											X	X
2.15.15	X	X	X	X																	X	X
2.15.16	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X
2.15.17 *(fed gov't reqmt)*																	X				X	X
2.15.18																						
2.15.19 *(fed gov't reqmt)*																						
2.15.20 *(fed gov't reqmt)*																						
2.15.21							X	X									X					
2.15.22																	X		X			
2.15.23																			X	X	X	X
2.15.24																				X	X	X
2.15.25	X	X	X	X													X		X	X	X	X
2.15.26	X	X	X	X								X	X	X	X	X	X	X	X	X	X	X
2.15.27							X										X		X			X
2.16.2	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
2.16.3	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
2.16.4	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
2.16.15	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
2.16.16							X	X					X	X	X	X		X		X	X	X
2.18.5	X	X	X	X			X					X	X	X	X	X	X	X		X	X	X

3.7 ADDITIONAL CONSIDERATIONS

3.7.1 All-Hazards Approach

In its broadest sense, cyber security for the power industry covers all issues involving automation and communications that affect the operation of electric power systems and the functioning of the utilities that manage them. This includes the goals of preventing, preparing for, protecting against, mitigating, responding to, and recovering from cyber events. In the power industry, the focus has been on implementing equipment that can improve power system reliability. Until recently, communications and IT equipment were typically seen as supporting power system reliability. However, increasingly these sectors are becoming more critical to the reliability of the power system. For example, with the exception of the initial power equipment problems in the August 14, 2003 blackout, the on-going and cascading failures were primarily due to problems in providing the right information to the right place within the right time. Also, the IT infrastructure failures were not due to any terrorist or Internet hacker attack; the failures were caused by inadvertent events – mistakes, lack of key alarms, and poor design. Therefore, inadvertent compromises must also be addressed and the focus must be an all-hazards approach.

3.7.2 Threat Categories

Threats can be allocated to one of the following three categories.

- The **manmade deliberate threat** focuses on incidents that are either enabled or deliberately caused by human beings with malicious intent, e.g., disgruntled employees, hackers, nation-states, organized crime, terrorists, and industrial spies.
- The **manmade unintentional threat** focuses on incidents that are enabled or caused by human beings without malicious intent, e.g., careless users and operators/administrators that bypass the security controls.
- The **natural threat** focuses on non-manmade incidents caused by biological, geological, seismic, hydrologic, or meteorological conditions or processes in the natural environment, e.g., earthquakes, floods, fires, and hurricanes.

This information is useful in assessing the extent of the impact and the subsequent forensic analysis.

3.7.3 Defense-in-Depth Strategy

Security is best applied in layers, with one or more security measures implemented at each layer. The objective is to mitigate the risk of one component of the defense being compromised or circumvented. This is often referred to as “defense-in-depth”. A defense-in-depth approach focuses on defending the network and attendant infrastructures through layered defenses (e.g., firewalls, intrusion detection systems, anti-virus software, and cryptography).

Because of the large variety of communication methods and performance characteristics, as well as because no single security measure can counter all types of threats, it is expected that multiple levels of security measures will be implemented.

3.7.4 Additional Requirements Selection Criteria

Additional criteria must be used in determining the cyber security requirements before selecting the cyber security measures. These additional criteria must take into account the characteristics of the interface, including the constraints and issues posed by device and network technologies, the existence of legacy systems, varying organizational structures, regulatory and legal policies, and cost criteria.

Once these interface characteristics are applied, then cyber security requirements can be applied that are both specific enough to be applicable to the interfaces, while general enough to permit the implementation of different cyber security solutions that meet the cyber security requirements or embrace new security technologies as they are developed. This cyber security information can then be used in subsequent steps to select cyber security controls for the Smart Grid.

3.7.5 Use of Existing Power Technologies to Address the Cyber Security Requirements

Power system operations have been managing the reliability of the power grid for decades in which availability of power has been a major requirement, with the integrity of information as a secondary but increasingly critical, requirement. Confidentiality of customer information has also been important in the normal revenue billing processes. Although focused on inadvertent security problems, such as equipment failures, careless employees, and natural disasters, many of the existing methods and technologies can be expanded to address deliberate cyber security attacks and security compromises resulting from the expanded use of IT and telecommunications in the electric sector.

One of the most important security solutions is to utilize and augment existing power system technologies to address new risks associated with the Smart Grid. These power system management technologies (e.g., SCADA systems; EMS; contingency analysis applications; fault location, isolation, and restoration functions; as well as revenue protection capabilities) have been refined for years to address the increasing reliability requirements and complexity of power system operations. These technologies are designed to detect anomalous events, notify the appropriate personnel or systems, continue operating during an incident/event, take remedial actions, and log all events with accurate timestamps.

In the past, there has been minimal need for distribution management except for load shedding to avoid serious problems. In the future, with generation, storage, and load on the distribution grid, utilities will need to implement more sophisticated power-flow-based applications to manage the distribution grid. Also, AMI systems can be used to provide energy-related information and act as secondary sources of information. These power-flow-based applications and AMI systems could be designed to address security.

Finally, metering has addressed concerns about confidentiality of revenue and customer information for many years. The implementation of smart meters has increased those concerns. However, many of the same concepts for revenue protection could also be used for the Smart Grid.

To summarize, expanding existing power system management capabilities to cover specific security requirements, such as power system reliability, is an important area for future analysis.

3.7.6 Implementation-Specific Solutions

Cyber security solutions must ultimately be implementation-specific, driven by the security requirements for the overall system. However, typical security requirements can be developed and used as checklists for actual implementations.

In the Smart Grid, the complexity of stakeholders, systems, devices, networks, and environments precludes implementing IT security techniques, only. Therefore, additional criteria must be used in selecting the cyber security measures. These additional criteria must take into account the constraints posed by device and network technologies, legacy systems, organizational structures, regulatory and legal policies, and cost criteria. These criteria should also take advantage of the existence of sophisticated equipment and systems that are already being used in the power system industry.

3.7.7 Additional Security Requirements

There are additional security requirements that will be applicable for the Smart Grid:

- Encrypting critical security parameters (CSPs). This could include sensitive configuration information, passwords, and cryptographic keys.
- Addressing end-point security and data at rest, for example, sensitive information in portable laptops.
- Implementation of a mutual distrust architecture to address potential compromises.
- Addressing the insider threat.
- Isolation of devices/components that have been compromised.

These will be discussed in the next draft of this document.

3.8 AREAS TO BE COVERED IN THE NEXT DRAFT OF THIS DOCUMENT

3.8.1 Combined Cyber-Physical Attacks

The smart grid is vulnerable to coordinated cyber-physical attacks against its infrastructure. Assessing the impact of coordinated cyber-physical attacks will require a sound, risk-based approach because the smart grid will inherit all of the physical vulnerabilities that the current power grid has (e.g., power outages caused by squirrels). Mitigating physical-only attacks is beyond the scope of this document, which is primarily focused on new risks and vulnerabilities associated with incorporating smart grid technologies into the existing power grid. The current version of this document is focused on assessing the impact of cyber-only vulnerabilities. Future versions of this document will assess the impact of coordinated cyber-physical attacks and revise the baseline impact levels presented in Table 3.3 – Power System Reliability Impact Levels, as needed.

3.8.2 Additional Areas for Analysis

As stated throughout this document, there are several topics that will be addressed in the next draft of this document. Following is a list of some of these topics:

- Design considerations to aid readers in using this document
- Tailoring of specific security requirements

- Currently, physical security is outside of the scope of this document. This will be reviewed for the final version of this document.

CHAPTER FOUR
PRIVACY AND THE SMART GRID

The SGIP-CSWG Privacy Sub-group conducted a privacy impact assessment (PIA) for the consumer-to-utility portion of the Smart Grid. In the months following the PIA, the group additionally considered the privacy impacts and risks throughout the entire Smart Grid structure, and also began to conduct an overview of the laws, regulations and standards[22] relevant to the privacy of energy consumption data. The focus of the Privacy group has been on what data may be collected or created that can reveal information about individuals or activities within specific premises (both residential and commercial), how these different types of information may be exploited, and policies and practices to identify and mitigate risks.

While the evolving Smart Grid will present societal benefits in the form of energy efficiency and grid reliability, it also presents potential privacy risks. The ability to access, analyze and respond to much more precise and detailed data from all levels of the electric grid is critical to the major benefits of the Smart Grid, and it is also a significant concern from a privacy viewpoint, especially when this data, and data extrapolations, are associated with individual consumers or locations. Some media articles have raised serious concerns[23] about the type and amount of billing, usage, appliance and other related information flowing throughout the various components of the Smart Grid.

There are also concerns across multiple industries about data aggregation of "anonymized" data[24]. For example, in other situations, taking multiple pieces of "anonymized" data has been shown by various studies to actually reveal specific individuals.[25] Frequent meter readings may provide not only a detailed time-line of activities occurring inside a metered location (see Figure 4.1), they could also lead to knowledge being gained about specific equipment usage or other internal business processes.

[22] See Appendix E for a preliminary list of state laws and regulations applicable to the electric sector.

[23] One example of this is available at http://www.philly.com/inquirer/business/20090906_Utilities__smart_meters_save_money__but_erode_privacy.html

[24] http://epic.org/privacy/reidentification/

[25] For one example of such a study, see the technical paper, "Trail Re-identification: Learning Who You are From Where You Have Been" by Bradley Malin, Latanya Sweeney and Elaine Newton, abstract available at http://privacy.cs.cmu.edu/people/sweeney/trails1.html.

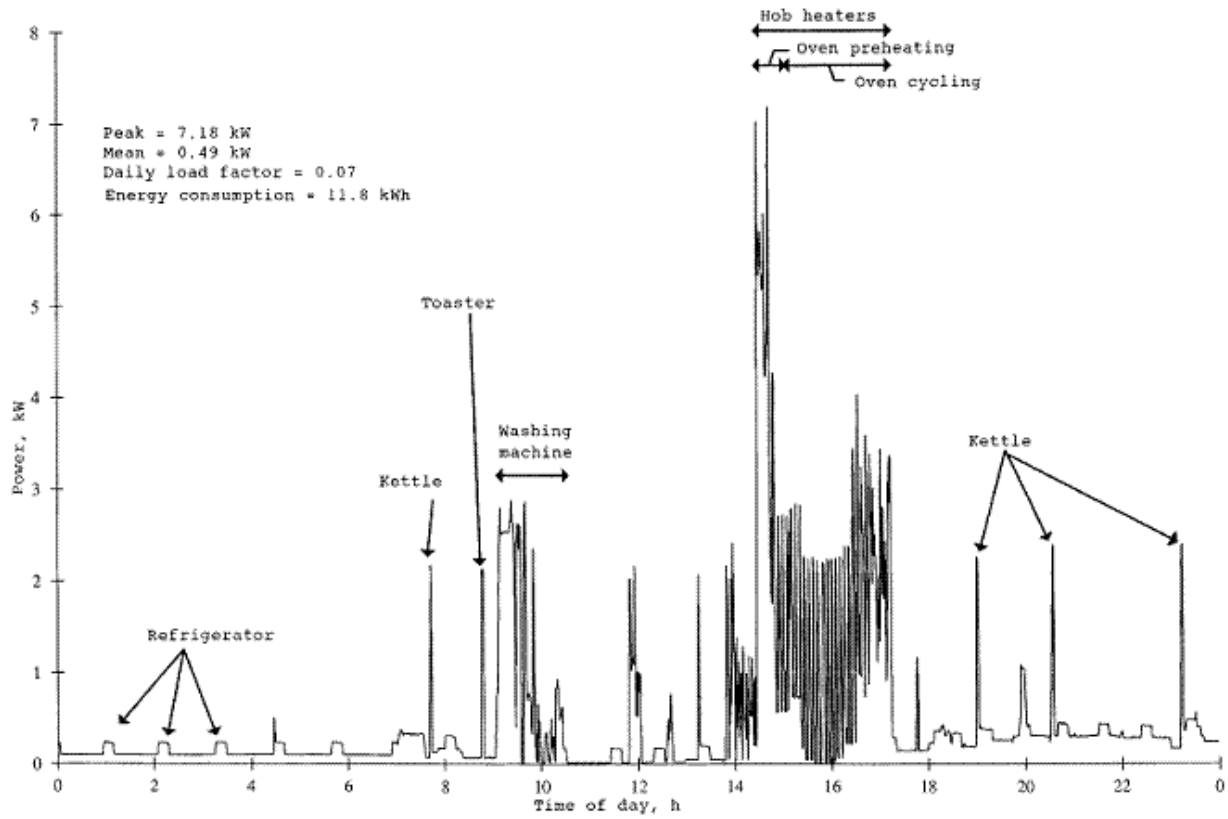

Figure 4.1 – How power use can reveal personal activities[26]

Smart meter data raises potential surveillance possibilities posing physical, financial and reputational risks. More data, and more detailed data, may be collected, generated and aggregated through Smart Grid operations than previously collected through monthly meter readings and distribution grid operations. (See Figure 4.2 for the NIST conceptual model) In addition to utilities, new entities may also seek to collect, access, and use smart meter data (e.g., vendors creating applications and services specifically for smart appliances, smart meters and other building-based solutions.)

[26] Elias Leake Quinn, *Smart Metering & Privacy: Existing Law and Competing Policies, Spring 2009*, pg. 3. Available at http://www.dora.state.co.us/puc/DocketsDecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf.

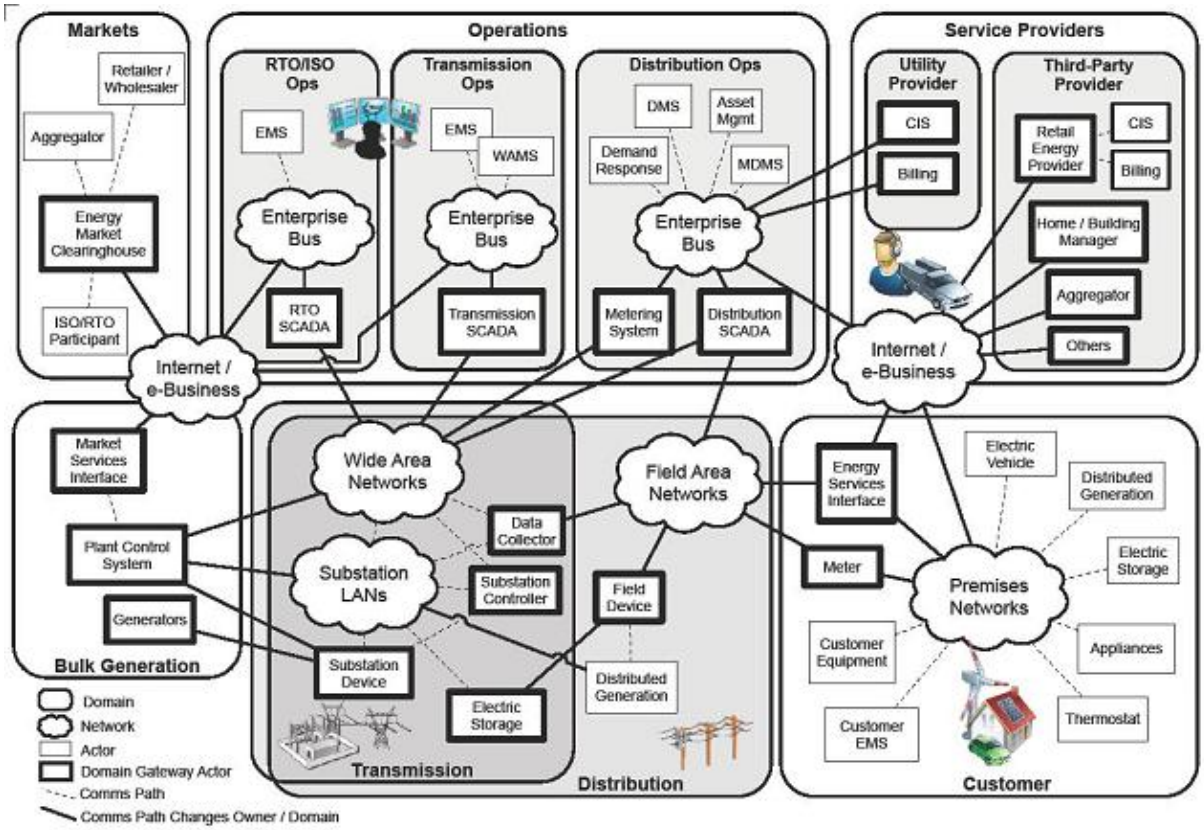

Figure 4.2 NIST Conceptual Model[27]

The proliferation of smart appliances and utility devices throughout the grid, on both sides of the meter, means an increase in the number of devices that may generate data. The privacy risks presented by these smart appliances and devices on the customer side of the meter are expanded when these appliances and devices transmit data outside of the Home Automation Network (HAN) or building management system and do not have documented security requirements, effectively extending the perimeter of the system beyond the walls of the premises.

Data may also be collected from electric vehicles and plug-in hybrid electric vehicles (EVs/PHEVs). Charging data may be used to track the travel times and locations for the EV/PHEV owners.

These risks may be addressed by policies and practices that are implemented with the evolution of the Smart Grid. During July and August of 2009 the Privacy subgroup of the SGIP-CSWG conducted an initial Privacy Impact Assessment (PIA) for the consumer-to-utility portion of the Smart Grid and an overview of the laws, regulations and standards relevant to the privacy of information related to consumers' personal energy consumption.

The following questions were identified and addressed in the process of performing the PIA and in the follow-on discussions of the findings:

[27] *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* Available at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf.

- What personal information may be generated, stored, transmitted or maintained by the Smart Grid?
- How is this information new or unique from personal information in other types of systems and networks?
- What are the new and unique types of privacy risks that may be created by Smart Grid components and entities throughout the grid network?
- Do existing laws, regulations and standards apply to the personal information collected by, created within, and flowing through the Smart Grid components?
- What could suggested privacy practices look like for all entities using the Smart Grid so that following them would protect privacy, reduce risks, and support and/or enhance existing laws, regulations and standards?

4.1 HIGH-LEVEL SMART GRID CONSUMER-TO-UTILITY PRIVACY IMPACT ASSESSMENT (PIA) REPORT

This Privacy Impact Assessment (PIA) was performed in accordance with numerous U.S. federal data protection requirements, and with the Organisation for Economic Cooperation and Development (OECD) Privacy Principles as outlined within the American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP). It also included consideration of global privacy protection laws, regulations and standards.

4.1.1 Summary of PIA Findings

The preliminary PIA results indicate that significant areas of concern remain to be addressed within each localized domain of the Smart Grid.

While some states have examined the privacy implications of the Smart Grid, most states have little or no documentation available. Furthermore, enforcement of state privacy-related laws is often delegated to agencies other than public utility commissions, who have regulatory responsibility for electric utilities. Research indicates that, in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid[28]. Comprehensive and consistent definitions of privacy-affecting information with respect to the Smart Grid typically do not exist at state or Federal regulatory levels, or within the utility industry[29]. Accordingly, there may be opportunities to develop processes and practices to identify and address privacy risks.

4.1.2 PIA Methodology

In developing this high-level PIA, the available documentation for use cases[30], covering the interactions between the consumers of services and the providers of those services, was reviewed

[28] Most public utility commissions do have significant customer privacy policies that pre-date the smart grid, which utilities take very seriously.

[29] Edison Electric Institute, the trade association of investor-owned electric utilities, is developing a formal position on customer data access, which it expects to finalize during 2010.

[30] http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/AugustWorkshop/All_of_the_Diagrams_in_one_document.pdf

against the OECD Privacy Principles[31] and the Generally Accepted Privacy Principles (GAPP)[32], which form the basis of most international, national and local data protection laws, along with consideration of safeguards as found in the international information security standard ISO/IEC 27001, also widely used for data protection regulatory compliance.

The following privacy principles were developed using the principles from the OECD Privacy Principles, the GAPP, and principles from ISO/IEC 27001. These are very general privacy principles designed to be applicable across a broad range of industries. They are not mandatory requirements.

Following each of the privacy principles are the related findings from the PIA. Following each of the findings are suggested privacy practices that may serve as mitigations for the concerns associated with each principle. If an organization has existing privacy responsibilities, policies, and procedures defined, the organization should consider reviewing, updating, and potentially augmenting these responsibilities, policies, and procedures to address the new privacy issues associated with the Smart Grid.

4.1.3 Principles, Findings, and Privacy Practices

1. **Management and Accountability:** An organization should consider formally appoint personnel to ensure that information security and privacy policies and practices should exist and are followed. Documented requirements for regular training and ongoing awareness activities should exist and be followed. Audit functions should be present to monitor all data accesses and modifications.

   Finding:

   Utilities should verify the existence of documented privacy responsibilities and authority within the organization.

   Suggested Privacy Practices:

   - **Assign privacy responsibility.** Each organization collecting or using energy usage data from or about premises should formally augment responsibility to a position or person to ensure that privacy policies and practices exist and are followed. As part of their augmented responsibilities, documented requirements for regular training and ongoing awareness activities should exist and be implemented. Audit functions should also be modified to monitor all data accesses and modifications of energy usage data.
   - **Establish law enforcement request policies and procedures**. For any organization accessing, storing, or processing energy usage data, the organization's incident response program should include specific procedures for energy usage data, as the Smart Grid is further deployed.

[31] OEDC Privacy Principles: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[32] GAPP http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles.htm

2. **Notice and Purpose:** A clearly-specified notice should exist and be shared in advance of the collection, use, retention, and sharing of energy usage data and personal information.

   Finding:

   The data obtained from Smart Grid systems and accompanying potential and actual uses for that data create the need for organizations to be more transparent and clearly provide notice documenting the types of information items collected, and the purposes for collecting the data.

   Suggested Privacy Practices:

   - **Provide notification for the personal information collected**. Any organization collecting energy usage data from or about premises should consider validating or adopting a process to notify the premises' inhabitants, and person(s) paying the bills (which may be different entities) when appropriate, of the data being collected, why it is necessary to collect the data, and describe the use, retention, and sharing of the data. This notification should consider including information about when and how information may or may not be shared with law enforcement officials. Data subjects should be told this information before the time of collection.
   - **Provide notification for new information use purposes and collection.** Organizations should consider updating customer notifications whenever an organization wants to start using existing collected data for materially different purpose than the customer has authorized. Also, organizations should notify the recipients of services whenever any organization wants to start collecting additional data beyond that already being collected, along with providing a clear explanation for why the additional data is necessary.

3. **Choice and Consent:** The organization should describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of their personal information.

   Finding:

   Currently it is not readily apparent that utilities or other entities within the Smart Grid obtain consent to use the personal information generated and collected for purposes other than billing. As smart meters increase capabilities and expand sharing of the data throughout the Smart Grid network, organizations should consider giving residents a choice about the types of data collected and how it is used.

   Suggested Privacy Practice:

   - **Provide notification about choices.** This notification should include a clearly worded description to the recipients of services notifying them of (1) any choices available to them about information being collected, and obtaining explicit consent when possible; and (2) explain why data items are being collected and used without obtaining consent from the individual (for example, needing certain pieces of information to restore service in a timely fashion).

4. **Collection and Scope:** Only personal information that is required to fulfill the stated purpose should be collected from individuals. Treatment of the information should conform to these privacy principles.

   Finding:

   In the current operation of the electric grid, data taken from meters consists of basic data usage readings required to create bills. Under a Smart Grid implementation, other types of data may be collected. Some of this additional data may be personal information. Because of the associated privacy risks, only the minimum amount of data necessary for service, provision and billing should be collected. Home power generation services will likely increase the amount of information created and shared.

   Suggested Privacy Practices:

   - **Limit the collection** of data to that necessary for grid operations, including planning and management, improving energy use and efficiency, account management and billing.

5. **Use and Retention:** Information should only be used or disclosed for the purpose for which it was collected, and should only be divulged to those parties authorized to receive it. Personal information should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. Personal information should only be kept as long as is necessary to fulfill the purposes for which it was collected.

   Finding:

   In the current operation of the electric grid, data taken from meters is used to create residents' bills, determine energy use trends, and allow customers to control their energy usage both on-site and remotely. The Smart Grid will provide data that can be used in ways not possible currently.

   Suggested Privacy Practices:

   - **Review privacy policies and procedures**. Any organization collecting energy usage data from or about premises should review existing privacy policies to determine how they may need to be modified. This review should include privacy policies already in place in other industries that may provide a model for the Smart Grid.

   - **Limit information retention**. Data, and subsequently created information that reveals personal information or activities, from and about specific premises should be retained only for as long as necessary to fulfill the purposes that have been communicated to the recipients of services. When no longer necessary, consistent with data retention and destruction requirements, the data and information, in all forms, should be irreversibly destroyed. This becomes more important as energy usage data becomes more granular, more refined, and has more potential for commercial uses.

6. **Individual Access:** Organizations should provide a process for personal information data subjects to allow them to ask to see their corresponding personal information and to

request the correction of perceived inaccuracies. Personal information data subjects should be informed about parties with whom personal information has been shared.

Finding:

In the current operation of the electric grid, data may be manually read from the meters. Consumers also have the capability to read the meter. Under a Smart Grid implementation, data may be stored in multiple locations to which the consumer may not have ready access.

Suggested Privacy Practice:

- **Customer access**. Any organization collecting energy usage data from or about premises should provide a process to allow service recipients access to the corresponding data from their specific premises, generated through their energy use and on their utilities account, and have dispute resolution procedures.

7. **Disclosure and Limiting Use:** Personal information should be used only for the purposes for which it was collected. Personal information should not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the service recipient.

Finding:

As Smart Grid implementations collect more granular and detailed information, this information is potentially revelatory of activities and equipment usage in a given location. As this information may reveal business activities, manufacturing procedures, and personal activities, significant privacy concerns and risks arise when the information is disclosed without the knowledge, consent and authority of the individual or organization to which the information applies.

Suggested Privacy Practice:

- **Limit information use.** Data on energy or other service usage obtained from Smart Grid operations should only be used or disclosed for the authorized purposes for which it was collected, and should only be divulged to or shared with those parties authorized to receive it and with whom the organizations have told the recipients of services it would be shared. This becomes more important as energy usage data becomes more granular, more refined, and has more potential for commercial uses.

8. **Security and Safeguards:** Personal information, in all forms, should be protected from loss, theft, unauthorized access, disclosure, copying, use, or modification.

Finding:

Data on energy or other service usage may be transmitted to and stored in multiple locations throughout the Smart Grid. Establishing strong security safeguards may be necessary to protect the collected data from loss, theft, unauthorized access, disclosure, copying, use, or modification.

Suggested Privacy Practices:

- **Associate energy data with individuals only when and where required**, for example only linking equipment data with a location or customer account when needed for billing, service restoration, or other operational needs. This practice is already common in the utility industry, and should be maintained and applied to other entities obtaining or using this data as the Smart Grid is further deployed.
- **De-identify information**. Usage data and any resulting information, such as monthly charges for service, collected as a result of Smart Grid operations should be aggregated and anonymized by removing personal information elements wherever possible to ensure usage of data from individual premises is limited appropriately. This may not be possible for some business activities, such as for billing.
- **Safeguard personal information**. Any organizations collecting, processing or handling energy usage data and other personal information from or about premises should ensure that all information collected and subsequently created about the recipients of services is appropriately protected in all forms from loss, theft, unauthorized access, disclosure, copying, use or modification. This practice is common in the utility industry; however, as other entities may have commercial uses for this information, these requirements should be reviewed by these other entities. In addition, given the growing granularity of information from Smart Grid operations, the responsibility for these existing policies should be reviewed and potentially augmented.
- **Don't use personal information for research purposes**. Any organization collecting energy usage data and other personal information from or about premises should refrain from using actual consumer personal information for research. There is currently and will be a great deal of research being conducted both inside and outside the utility industry on the Smart Grid, its effect upon demand response, and other topics. The use of actual information that can be linked to a consumer in this research would increase the risk of inadvertent exposure.

9. **Accuracy and Quality:** Every effort should be made to ensure that the data usage information is accurate, complete, and relevant for the purposes identified in the notice, and remains accurate throughout the life of the data usage information while within the control of the organization.

Finding:

The data collected from smart meters and related equipment will potentially be stored in multiple locations throughout the Smart Grid. Smart Grid data may be automatically collected in a variety of ways. Establishing strong security safeguards will be necessary to protect the information. Since Smart Grid data may be stored in many locations, and therefore, accessed by many different individuals and entities and used for a very wide variety of purposes, personal information may be inappropriately modified. Automated decisions about home energy use could be detrimental for residents (e.g., restricted power, thermostats turned to dangerous levels), while decisions about personal energy consumption could be based upon inaccurate information.

Potential Privacy Practice:

- **Keep information accurate and complete**. Any organization collecting energy usage data from or about premises should establish formal policies and procedures to ensure that the Smart Grid data collected from, and subsequently created about recipients of services, is accurate, complete and relevant for the purposes identified for which they were obtained, and remains accurate throughout the life of the Smart Grid data within the control of the organization.

10. **Openness, Monitoring, and Challenging Compliance:** Privacy policies should be made available to service recipients. These service recipients should be given the ability and process to challenge an organization's compliance with their state privacy regulations and organizational privacy policies as well as their actual privacy practices.

Finding:

In the current electric grid, utilities follow a wide variety of methods and policies for communicating to service recipients how personal information is used. The data collected from new smart meters and related equipment will potentially be stored in multiple locations throughout the Smart Grid, possibly within multiple states. This complicates the openness of organizational privacy compliance and being able to challenge the organization's compliance with privacy policies and practices.

Suggested Privacy Practices:

- **Policy challenge procedures**. Organizations collecting energy usage data, and all other entities throughout the Smart Grid, should establish procedures that allow service recipients to have the ability and process to challenge the organization's compliance with their published privacy policies as well as their actual privacy practices. This becomes more important as energy usage data becomes more granular, more refined, and has more potential for commercial uses.
- **Perform regular privacy impact assessments**. Any organization collecting energy usage data from or about premises should consider performing annual PIAs, and providing a copy of the results to each involved state's public utilities commissioner's office to review. This will help to assure compliance with appropriate state policies and provide an accessible public record. Organizations should also perform a PIA on each new system, network, or Smart Grid application and consider providing a copy of the results to each involved state's public utilities commissioner's office to review.
- **Establish breach notice practices.** Any organization collecting energy usage data from or about premises should consider expanding or establishing policies and procedures to identify breaches and misuse of Smart Grid data, along with expanding or establishing procedures and plans for notifying service recipients in a timely manner with appropriate details about the breach. This becomes particularly important with new possible transmissions of billing information between utilities and other information between utilities and other entities providing services in a smart grid environment (e.g.,. third party energy efficiency service providers).

4.2 PERSONAL INFORMATION IN THE SMART GRID

Personal information reveals something, either explicitly or implicitly, about specific individuals, groups of individuals, or activities of those individuals.

Data potentially maintained by organizations utilizing the Smart Grid such as energy usage, as well as increased frequency of usage reporting, or appliance or device reporting on energy consumption provide new sources of personal information. Traditional personal information collected by utility companies can be used to identify individuals including house number and/or address, homeowner or resident's first, middle, or last name, date of birth, and last four digits of the social security number (SSN). Smart Grid data elements combined with traditional personal information data elements reflecting the timing and amount of energy used can provide insights into life style (residential customers) and business operations (commercial and industrial customers). With a few exceptions, such as SSN and credit card numbers, rarely does a single piece of information or a single source lead to identification of an individual or group of individuals.[33] The concern is that combining data from another source with seemingly anonymous Smart Grid data might lead to identifying individuals or groups of individuals associated with an address.[34] Computing technology can make this much easier.

For example, Latanya Sweeney, a computer science professor and leading researcher on the topic of data re-identification, notes that combining census data elements such as zip code, birth date, and sex with other data sets with the same information can allow for the re-identification of data subjects.[35] Sweeney's study gathered data from the Massachusetts Group Insurance Commission (GIC). GIC, which purchases health insurance for state employees, released insurer records to researchers. GIC, with the support of the Governor's office, removed names, addresses, social security numbers, and other identifying information in order to protect the privacy of the employees. Sweeney then purchased voter rolls, which included the name, zip code, address, sex, and birth date of voters in Cambridge. From GIC's databases, only six people in Cambridge were born on the same day as the governor, half of them were men, and the governor was the only one who lived in the zip code provided by the voter rolls. The information in the GIC database on the Massachusetts governor included prescriptions and diagnoses.

Another study conducted in 2008 illustrates the increasing ease of de-anonymizing and aggregating data into personally identifiable information. Carnegie Mellon professors Alessandro Acquisti and Ralph Gross assessed the predictability of SSNs by knowing the date and geographic location of that individual's birth.[36]

These two cases show that data could be re-identified by combining two data sets with different types of information about an individual, but contain the same types of PII data in common. One

[33] http://www.cs.colostate.edu/~cs656/presentations-2009/HeYan-kAnonimity.ppt

[34] http://usacm.acm.org/usacm/VRD/

[35] L. Sweeney, *Uniqueness of Simple Demographics in the U.S. Population*, LIDAPWP4. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA: 2000.

[36] Alessandro Acquisti1 and Ralph Gross, Predicting Social Security numbers from public data, May 5, 2009, http://www.pnas.org/content/106/27/10975.full.pdf+html

of the data sets contained anonymized information; the other contained outside information–generally available to the public–collected on a routine basis, which included identifying information. If both datasets have at least one type of information that is the same, the anonymized information may be linked to an individual, or may narrow the possibilities to the point that linkage is trivial. While current privacy and security practices tend to focus on the removal of personally identifiable information (PII), the studies above show that re-identification can occur. This issue of data re-identification becomes potentially much more significant as the amount and granularity of the data being gathered during Smart Grid operations increase as more components of the Smart Grid are deployed.

Table 4.1 identifies potential data and descriptions of information that may be available in the Smart Grid.

Table 4.1 – Information potentially available through the Smart Grid

Data Element(s)	Description
a. Name	Party responsible for the account
b. Address	Location where service is being taken
c. Account Number	Unique identifier for the account
d. Meter reading	kW, kWh consumption recorded at 15-60 minute intervals during the current billing cycle
e. Current bill	Current amount due on the account
f. Billing history	Past meter reads and bills, including history of late payments/failure to pay, if any
g. Home area network	In-home electrical appliances
h. Lifestyle	When the home is occupied and unoccupied, when occupants are awake and asleep, how much various appliances are used
i. Distributed resources	The presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns
j. Meter IP	The Internet Protocol address for the meter, if applicable
k. Service provider	Identify of the party supplying this account, relevant only in retail access markets

4.3 PRIVACY CONCERNS

Privacy concerns about the Smart Grid may impact the implementation of Smart Grid systems or their effectiveness. For example, a lack of consumer confidence in the security and privacy of their energy consumption data may result in a lack of customer acceptance and participation, if not outright litigation.

In general, privacy concerns about the Smart Grid fall into one of two broad categories:

- Type I: Personal information not previously readily obtainable.

- Type II: Mechanisms for obtaining (or manipulating) personal information that did not previously exist.

Examples of Type I include detailed information on the appliances and equipment in use at a given location, and finely grained time series data on power consumption at metered locations and from individual appliances.

Type II includes instances where personal information is available from other sources, and the Smart Grid may present a new source for that same information. For example, an individual's physical location can be tracked through their credit card and cell phone records today. Charging EVs/PHEVs raises the possibility of tracking physical location through new energy consumption data.

4.3.1 Data Collection and Availability under Smart Grid

Detailed pictures of activities within a house or building can be derived from "equipment electricity signatures" and their time patterns. These can provide a basis for making assumptions about occupant activities, for example, the number of individuals at a premise, and when the location was unoccupied.

While technology to communicate directly with appliances and other energy consumption elements already exists, Smart Grid implementation may create broader incentives for their use. Appliances so equipped may deliver granular energy consumption to both their owners and operators, and to outside parties.

Table 4.2 outlines some of the possible areas of privacy concern, and provides some analysis of the nature of the concern according to the categories listed above. While this is not an exhaustive list, it serves to help categorize the concerns noted.

Table 4.2 – Potential Privacy Concerns and Descriptions

Privacy Concern	Discussion	Categorization
Fraud	Attributing energy consumption to another location or vehicle (in the case of EVs/PHEVs).	Type II: While fraud is an existing concern, the current system of reading customer meters (either manual recording or electronically via "drive-by" remote meter reading systems) would appear to allow less opportunity for data manipulation without collusion for the personnel collecting the data.
Determine Personal Behavior Patterns / Appliances Used	Smart meter and home automation network data may track the use of specific smart appliances. Access to data use profiles that can reveal specific times and locations of electricity use in specific areas of the home can also indicate the types of activities and/or appliances used. • Appliance manufacturers may want to	Type I: The type of data made available by Smart Grid implementation, which may be both more granular, and available on a broader scale.

Privacy Concern	Discussion	Categorization
	get this information to know who, how and why individuals used their products in certain ways. • Such information could impact appliance warranties. • Other entities may want this data to do targeted marketing.	
Perform Real-Time Remote Surveillance	Access to live energy use data can reveal if people are in a facility or residence, what they are doing, where they are in the structure, and so on.	Type II: Many methods of real-time surveillance currently exist. The availability of computerized real-time or near real-time energy usage data would create another way in which such surveillance could be conducted.
Non-Grid Commercial Uses of Data	Personal energy consumption data storage may reveal lifestyle information that could be of value to many entities including vendors of a wide range of products and services. • Vendors may purchase attribute lists for targeted sales and marketing campaigns that may not be welcomed by those targets.	Under the existing metering and billing systems, meter data is not sufficiently granular in most cases to reveal any detail about activities. However, smart meters, time of use and demand rates, and direct load control of equipment may create detailed data which could be sold and used for energy management analyses and peer comparisons. While this information has beneficial value to third parties, consumer education about protecting that data has considerable positive outcomes.

4.3.2 Mitigating Factors

Many of the concerns relating to Smart Grid and privacy may be addressed by limiting the information required to that which is necessary from an operational standpoint.

Where there is an operational need for information, controls should be implemented to ensure that data is collected *only* where such a need exists. Organizations may want to develop policies to determine what customer and premises information should be confidential and how that information should be retained, distributed internally and secured from breach. As noted in other parts of this document, training employees is critical to implementing this policy. Similarly, service recipients should be informed as to what information the organization is collecting and how that information will be used. Service recipients may also need the ability to inspect that information for accuracy and quality, as recommended in the privacy principles listed above.

Existing business rules, standards, laws and regulations previously considered applicable to other sectors of the economy might be usable as models to provide protection against Type II areas of concern. However, because of the current technology used for the collection of the data, Type I concerns may require new rules of business, standards or regulation. These issues are discussed in more detail in the following sections.

4.4 SOME NEW PRIVACY CONSIDERATIONS FOR THE SMART GRID

Data collections in the Smart Grid pose a unique setting. Large scale deployment of some Smart Grid components can be expected to happen very rapidly. Currently, it is not consistently defined across the country who owns what data. In addition, the measurements go into the heart of users' private sphere, potentially giving precise information about their behavior in the privacy of their homes. Two aspects of the Smart Grid data need to be considered in the review of existing laws and regulatory policies to ensure that new types of data are addressed:

1. Granular and available data on use of individual appliances by time and location.
2. Public awareness of contractual agreements about data ownership and what may be revealed about people's daily activities.

4.4.1 Granularity of Energy Consumption Data

It appears that no laws currently explicitly cover privacy protection for appliance energy usage data, but keeping appliance data may take on increased legal importance. Energy consumption data may create new opportunities to monitor energy consumption to the benefit, or harm, of consumers and businesses, especially if data is collected for a long enough time to allow for advanced statistical methods to be applied. A beneficial example would be a furnace manufacturer monitoring energy data to note that a furnace was no longer functioning efficiently, and therefore in need of either maintenance or replacement. A harmful example would be a competing furnace manufacturer obtaining that same information and representing it as evidence to highlight advantages of their product.

4.4.2 Data Ownership

This is in many ways similar to data obtained by a car rental company regarding the timing and location of your car rental. They own the data, and it could reveal potentially embarrassing or harmful information about your activities. But you have, in signing your rental agreement, agreed to their ownership of the data, so there is no new legal ground here. However, the ramifications of the extent to which Smart Grid data can reveal consumer behaviors are unknown to the majority of the U.S. population. Similar to the issues that arose as Facebook users discovered that personal information was disseminated beyond their intended group of friends, consumers could benefit from education about the value of energy consumption data so they exercise caution in its use. Existing consumer protection laws and regulatory policies may need to be examined to ensure that these can extend to Smart Grid energy consumption data. Additional problems may be the lack of fine grained choice for users (one can simply not rent a car, but cannot opt out of the Smart Grid). An additional complication is the number of organizations that potentially could claim data ownership: for example, a house owner rents a room to a student (whose boyfriend is charging his electrical vehicle at her place), the same house owner subscribes to an energy savings service, and the applicable power company outsources the data processing to a third party overseas.

4.5 SMART GRID PRIVACY SUMMARY

The Privacy group reached the following conclusions:

1. The evolving Smart Grid technologies and associated new types of information related to individuals and premises may create privacy risks and challenges that are not addressed or mitigated by existing laws and regulations with regard to energy consumption, billing and other related Smart Grid data.

2. New Smart Grid technologies, and particularly smart meters and similar types of endpoints, may also create new privacy risks and concerns beyond the existing practices and policies of the organizations that have been historically responsible for protecting energy consumption data collected from the traditional electrical grid.

Given these realities and findings, it is hoped that the information contained in this chapter will serve as a useful guide and reference for the wide variety of Smart Grid domain players and lawmakers who have, or may have, responsibility for consumer energy consumption data now or at a future date.

CHAPTER FIVE
STANDARDS REVIEW

The 2007 EISA assigns NIST the responsibility to coordinate development of an interoperability framework including model standards and protocols. The identification of the standards and protocol documents that support interoperability of the Smart Grid is therefore a key element of the NIST framework. In this draft of the NISTIR, this chapter identifies the standards that the SGIP-CSWG has identified as relevant to cyber security in the Smart Grid. This list of standards represents what is currently being evaluated for inclusion in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards*. Work continues to identify other requirements that should be included in this chapter. In addition, the standards sub-group is reviewing the standards that have been identified at the NIST Smart Grid workshops and by the various PAP teams to determine whether each standard includes security requirements. Over the next few months, the list will be expanded to include all the standards identified by the PAP teams. Security requirements that are included in each standard will be compared to the requirements specified in this NIST report. In this draft of the NISTIR, the comparison focuses on the security families listed in the DHS Catalog. In the next version of the NISTIR, the comparison will be at the requirement level.

This chapter contains three tables: Table 5.1 provides an overview of each of the standards; Table 5.2 identifies the security families that are addressed by each standard; and Table 5.3 lists the applicable OSI layer and includes any additional notes.

The columns in the following tables represent:

- **ID Number** – for reference only so that other columns or discussions can easily make reference to the information for an item in this table
- **SDO** – identifies the Standard Developing Organization
- **Standard ID** – identifies the standard being referred to
- **Standard Name** – provides the detailed name of the standard
- **Working Group** – identifies the working group responsible for the standard development within the standard developing organization
- **Contact Name** – the name of the person who is the contact or liaison for the standard working group if applicable
- **Contact Email** – contact information for the working group contact
- **Standard Freely Available (Y/N)** – Identifies whether the standard can be obtained through the internet for download

- **Price** – identifies the price associated with purchasing and/or downloading the standard
- **Version Reviewed** – identifies the version that is being reviewed by the SGIP-CSWG for consideration in Smart Grid Security
- **Required by Regulation or Law (Y/N)** – identifies whether there is a governing body that deems this standard required
- **Utility Industry Specific (Y/N)** – indicates whether the standard is specific to the utility industry
- **Categories 2.1 – 2.18** – derived from the DHS catalogue categories – these columns identify whether the standard was a control of the specific catalogue category
- **OSI Stack Layers** – identifies which layers are involved in the standard
- **Notes and/or Comments** – provides additional detail or comments regarding the standard and its evaluation by the SGOP-CSWG

Reader Note: Not all standards listed are currently available to the SGIP-CSWG and therefore cannot be thoroughly documented. Any comments received from external parties regarding standards that the requirements sub-group does not have access to were not addressed.

5.1 STANDARDS DOCUMENT CHARACTERISTICS

The following table provides summary information of the preliminary list of the standards that are being reviewed by the standards working sub-group of the SGIP-CSWG.

Table 5.1 – Standards Overview

ID No.	SDO	Standard ID	Standard Name	Working Group	Standard Freely Available (Y/N)	Price	Version Reviewed	Required by Regulation or law (Y/N)	Utility Industry Specific (Y/N)
1	IEC	IEC 62351 -1	Data and Communications Security Part 1: Introduction to Security Issues	IEC TC57 WG15	Y	$ 143	V1	N	Y
2	IEC	IEC 62351 -2	Data and Communications Security	IEC TC57	Y	$ 204	V1	N	

ID No.	SDO	Standard ID	Standard Name	Working Group	Standard Freely Available (Y/N)	Price	Version Reviewed	Required by Regulation or law (Y/N)	Utility Industry Specific (Y/N)
			Part 2: Glossary of Terms	WG15					
3	IEC	IEC 62351 -3	Data and Communications Security Part 3: Profiles Including TCP/IP	IEC TC57 WG15	Y	$ 51	V1	N	Y
4	IEC	IEC 62351 -4	Data and Communications Security Part 4: Profiles Including MMS	IEC TC57 WG15	Y	$ 77	V1	N	Y
5	IEC	IEC 62351 -5	Data and Communications Security Part 5: Security for IEC 60870-5 and Derivatives	IEC TC57 WG15	Y	$ 204	V1	N	Y
6	IEC	IEC 62351 -6	Data and Communications Security Part 6: Security for IEC 61850	IEC TC57 WG15	Y	$ 77	V1	N	Y
7	IEC	IEC 62351 -7	Data and Communications Security Part 7: Network and system management (NSM) data object models	IEC TC57 WG15	When published		V1	N	Y
8	IEC	IEC 62351 -8	Data and Communications Security Part 8: Role-based access control	IEC TC57 WG15	When completed			N	Y
9	ANSI	ANSI C12.22	Meter and End Device Tables communications over any network	ANSI C12.22	N	$166	ANSI C12.22-2008	N	Y
10	DHS	DHS	Catalog of Control Systems Security: Recommendations for Standards Developers	DHS			V4	N	N
11	IEEE	IEEE 802.11i	Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements		Y		7/23/2004		N
12	IEEE	IEEE 1547.3	Guide For Monitoring, Information Exchange, and Control of Distributed	IEEE 1547.3	Y	$120	V1	N	Y

ID No.	SDO	Standard ID	Standard Name	Working Group	Standard Freely Available (Y/N)	Price	Version Reviewed	Required by Regulation or law (Y/N)	Utility Industry Specific (Y/N)
			Resources Interconnected with Electric Power Systems						
13	IEEE	IEEE 1686	Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities		N	$63 to $102	2007 (initial)	N	Y
14	IETF	SNMP	Simple Network Management Protocol (SNMP)	IETF	Y	$0	V3	N	N
15	ISA IEC	SP99 IEC 62443	Cyber security mitigation for industrial and bulk power generation stations	IECTC65	N				N
16	ISO	ISO 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary		N				N
17	NERC	CIP 002 thru 009	NERC Critical Infrastructure Protection (CIP Standards)		Y	$0	V2	Y	Y
18	NIST	FIPS 140-2	Security Requirements for Cryptographic Modules		Y	$0		N	N
19	NIST	FIPS 197	Cryptographic standard: Advanced Encryption Standard (AES)		Y	$0	11/26/2001	N	N
20	NIST	SP 800-53	Security controls required for federal information systems		Y	$0	2.0	N	N
21	NIST	SP 800-82	DRAFT Guide to Industrial Control Systems (ICS) Security		Y	$0	2nd Draft	N	N
22	IEC	IEC 61850-3	General electrical and security requirements for substation IEDs	IEC TC57 WG10	Y	$260	V1	N	Y
23	UCAIug	UCAIug AMI-SEC	System Security Requirements	AMI-SEC	Y	$0	1.01	N	Y

ID No.	SDO	Standard ID	Standard Name	Working Group	Standard Freely Available (Y/N)	Price	Version Reviewed	Required by Regulation or law (Y/N)	Utility Industry Specific (Y/N)
24	OASIS	WS-Security	Web Services Security	OASIS Web Services Security (WSS) TC	Y	$0	1.1		N
25	IEEE	802.1AR	Secure Device Identity		N	$100	2009	N	N
26	IEEE	802.1AE	Media Access Control Security Standard		Y	$0	2006	N	N
27	IEEE	802.1X-REV	Port Based Network Access Control		N	$102	D4.5	N	N
28	IETF	TLS	Transport Layer Security (TLS)		Y	$0	1.2/RFC5246	N	N
29	IETF	DTLS	Datagram Transport Layer Security (DTLS)		Y	$0	1.0/RFC4347	N	N
30	IETF	IPSec	Internet Protocol Security		Y	$0		N	N
31	IETF	RFC3711	Secure Real-Time Transport Protocol		Y	$0		N	N
32	IETF	RFC4962	Guidance for Authentication, Authorization, and Accounting (AAA) Key management		Y	$0		N	N
33	IETF	RFC 3748	Extensible Authentication Protocol (EAP)		Y	$0		N	N
34	IEEE	802.16e	Air Interface for Broadband Wireless Access Systems (WiMax)		N	$380	2009	N	N
35	NIST	SP 800-38(A-E)	Recommendations for Block Cipher modes		Y	$0			
36	3GPP	TS 33.102	UMTS LTE 3G Security Architecture		Y	$0	8.4.0	N	N
37	ISO/IEC	ISO/IEC 9798	Security Techniques - Entity Authentication (Parts 1 - 4)		N				N
38	ISO/IEC	ISO/IEC 11770	Security Techniques - Key Management		N				N

ID No.	SDO	Standard ID	Standard Name	Working Group	Standard Freely Available (Y/N)	Price	Version Reviewed	Required by Regulation or law (Y/N)	Utility Industry Specific (Y/N)
			(Parts 1 - 3)						
39	ISO/IEC	ISO/IEC 13888	Security Techniques - Non Repudiation (Parts 1 - 3)		N				N
40	ISO/IEC	ISO/iEC 14888	Security Techniques - Digital Signatures (Parts 1 - 3)		N				N
41	ISO/IEC	ISO/IEC 15946-1	Cryptographic Techniques Based on Elliptic Curves -Part 1:General		N	$122	2008		N
42	ISO/IEC	ISO/IEC 18033	Security Techniques - Encryption Algorithms (Parts 1 - 4)		N				N
43	ISO/IEC	ISO/IEC 19772	Security techniques -- Authenticated encryption		N	$116	2009		N
44	W3C	XML Encryption	XML Encryption Syntax and Processing		Y	$0		N	N
45	W3C	XML Signature	XML Signature Syntax and Processing		Y	$0		N	N
46	W3C	Canonical XML	Canonical XML		Y	$0		N	N
47	NERC CSSWG (1)[37]		Security Guidelines for the Electricity Sector: Control System Cyber Security Incident Response Planning		Y	$0	V 1.0 May 2, 2007	N	Y
48	NERC CSSWG (2)		Security Guidelines for the Electricity Sector: Control System — Business Network Electronic Connectivity		Y	$0	V 1.0 May 3, 2005	N	Y
49	NERC CSSWG (3)		Security Guidelines for the Electricity Sector: Patch Management for Control Systems		Y	$0	V 1.0 May 3, 2005	N	Y

[37] The number in parentheses for the five NERC CSSWG documents is for reference purposes only – to distinguish the five documents.

ID No.	SDO	Standard ID	Standard Name	Working Group	Standard Freely Available (Y/N)	Price	Version Reviewed	Required by Regulation or law (Y/N)	Utility Industry Specific (Y/N)
50	NERC CSSWG (4)		Security Guidelines for the Electricity Sector: Physical Security - Substations		Y	$0	V 1.0 October 15, 2004	N	Y
51	NERC CSSWG (5)		Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs		Y	$0	V0.995 December 3, 2009?	N	Y
52	IEEE	C37.231	Recommended Practice for Microprocessor-based Protection Equipment Firmware Control		N	$63.00	2006	N	Y
53	NIST	FIPS 198	The Keyed-Hash Message Authentication Code(HMAC)		Y	$0	3/6/2002		N
54	NIST	FIBS 180-2	Secure Hash Standard(SHS)		Y	$0	8/1/2002		N
55	ANSI	ANS X9.52-1998	Triple Data Encryption Algorithm Modes of Operation		N	$100	1998		N
56	NIST	FIPS 197	Advanced Encryption Standard(AES)		Y	$0	11/26/2001		N
57	NIST	FIPS 186-3	Digital Signature Standard(DSS)		Y	$0	Jun-09		N
58	ANSI	ANSI X9.62	Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm(ECDSA)		N	$100	2005		N
59	PKCS	PKCS #1,#3,#5-#12,#15	RSA Public Key Cryptography Standards		Y				N
60	ANSI	ANSI X9.42	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography		N	$100	2003		N
62	IETF	IETF 4120	The Kerberos Network Authentication Service (V5)		Y		Jul-05		N

ID No.	SDO	Standard ID	Standard Name	Working Group	Standard Freely Available (Y/N)	Price	Version Reviewed	Required by Regulation or law (Y/N)	Utility Industry Specific (Y/N)
63	ANSI/INCITS	INCITS 359	Information Technology - Role Based Access Control		N	$30	2/3/2004		N
64	NIST	SP 800-63	Electronic Authentication Guideline		Y	$0	April 2006	N	N
65	OASIS	XACML 2.0	eXtensible Access Control Markup Language	OASIS XACML TC	Y	$0	2.0	N	N
66	OASIS	SAML 2.0	Security Assertion Markup Language	OASIS Security Services TC	Y	$0	2.0	N	N
67	OGC	GeoXACML	Geospatial exTensible Access Control Markup Language (GeoXACML)	OGC Security Work Group	Y	$0	1.0	N	N

5.2 DHS CATALOG SECURITY FAMILIES

The following table lists the standards and an identification of the security families that are addressed by the standard. This is an initial high level assessment that will be revised.

Table 5.2 – Standards and Applicable Security Families

ID Number	SDO	Standard ID	2.1 Security Policy	2.2 Organizational Security	2.3 Personnel Security	2.4 Physical and Environmental Security	2.5 System and Services Acquisition	2.6 Configuration Management	2.7 Strategic Planning	2.8 System and Communication Protection	2.9 Information and Document Management	2.10 System Development and Maintenance	2.11 Security Awareness and Training	2.12 Incident Response	2.13 Media Protection	2.14 System and Information Integrity	2.15 Access Control	2.16 Audit and Accountability	2.17 Monitoring & Reviewing Control System Security Policy	2.18 Risk Management and Assessment
1	IEC	IEC 62351 -1											X							
2	IEC	IEC 62351 -2																		
3	IEC	IEC 62351 -3								X										
4	IEC	IEC 62351 -4								X										
5	IEC	IEC 62351 -5								X										
6	IEC	IEC 62351 -6								X										
7	IEC	IEC 62351 -7				X		X		X				X		X		X		
8	IEC	IEC 62351 -8									X						X			
9	ANSI	ANSI C12.22								X						X				
10	DHS	DHS	The DHS Catalog is a source document for the requirements in this NISTIR.																	
11	IEEE	IEEE 802.11i								X										
12	IEEE	IEEE 1547.3				X				X										
13	IEEE	IEEE 1686						X		X							X	X	X	
14	IETF	SNMP																	X	
15	ISA IEC	SP99 IEC 62443																		

ID Number	SDO	Standard ID	2.1 Security Policy	2.2 Organizational Security	2.3 Personnel Security	2.4 Physical and Environmental Security	2.5 System and Services Acquisition	2.6 Configuration Management	2.7 Strategic Planning	2.8 System and Communication Protection	2.9 Information and Document Management	2.10 System Development and Maintenance	2.11 Security Awareness and Training	2.12 Incident Response	2.13 Media Protection	2.14 System and Information Integrity	2.15 Access Control	2.16 Audit and Accountability	2.17 Monitoring & Reviewing Control System Security Policy	2.18 Risk Management and Assessment
16	ISO	ISO 27000																		
17	NERC	CIP 002 thru 009	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
18	NIST	FIPS 140-2	X							X										
19	NIST	FIPS 197								X						X				
20	NIST	SP 800-53	NIST SP 800-53 is a source document for the requirements in this NISTIR. Appendix B includes a mapping between NIST SP 800-53 and the DHS Catalog.																	
21	NIST	SP 800-82	5.5 General Firewall Policies for ICS	4 ICS Security Program Development & Deployment	6.2.1 Personnel Security	6.2.2 Physical & Environment Protection	6.1.3 System & Services Acquisition	6.2.4 Configuration Management	6.1.2 Planning	6.3.4 Systems & Communication Protection	6.3.2 Access Control	6.2.5 Maintenance	6.2.9 Awareness & Training	6.2.3 Contingency Planning, 6.2.8 Incident Response	6.2.7 Media Protection	6.2.6 System & Information Integrity	6.3.1 Identification & Authentication; 6.3.2 Access Control	6.3.3 Audit & Accountability	6.1.4 Certification, Accreditation, & Security Assessments	
22	IEC	IEC 61850-3								DHS 2.8.5						DHS 2.15.7				

ID Number	SDO	Standard ID	2.1 Security Policy	2.2 Organizational Security	2.3 Personnel Security	2.4 Physical and Environmental Security	2.5 System and Services Acquisition	2.6 Configuration Management	2.7 Strategic Planning	2.8 System and Communication Protection	2.9 Information and Document Management	2.10 System Development and Maintenance	2.11 Security Awareness and Training	2.12 Incident Response	2.13 Media Protection	2.14 System and Information Integrity	2.15 Access Control	2.16 Audit and Accountability	2.17 Monitoring & Reviewing Control System Security Policy	2.18 Risk Management and Assessment
23	UCAIug	UCAIug AMI-SEC	3.2.5 Boundary Services	3.4.2 Organizational Rigor	3.4.2 Organizational Rigor	3.4.2 Organizational Rigor	3.4.1 Development Rigor	3.4.1 Development Rigor	3.4.2 Organizational Rigor	3.2.10 Resource Management Services	3.2.9 Notification & Signaling Services	3.4.1 Development Rigor	3.4.2 Organizational Rigor	3.4.3 Handling/Operating Rigor	3.4.2 Organizational Rigor	3.1.2 Integrity	3.2.3 Authentication	3.2.2 Auditing	3.4.2 Organizational Rigor	N/A
24	OASIS	WS-Security													X	X				
25	IEEE	802.1AR								X							X			
26	IEEE	802.1AE								X							X			
27	IEEE	802.1X-REV								X							X			
28	IETF	TLS								X							X			
29	IETF	DTLS								X							X			
30	IETF	IPSec								X							X			
31	IETF	RFC3711								X										
32	IETF	RFC4962								X							X			
33	IETF	RFC 3748								X							X			
34	IEEE	802.16e								X							X			
35	NIST	SP 800-38(A-								X										

ID Number	SDO	Standard ID	2.1 Security Policy	2.2 Organizational Security	2.3 Personnel Security	2.4 Physical and Environmental Security	2.5 System and Services Acquisition	2.6 Configuration Management	2.7 Strategic Planning	2.8 System and Communication Protection	2.9 Information and Document Management	2.10 System Development and Maintenance	2.11 Security Awareness and Training	2.12 Incident Response	2.13 Media Protection	2.14 System and Information Integrity	2.15 Access Control	2.16 Audit and Accountability	2.17 Monitoring & Reviewing Control System Security Policy	2.18 Risk Management and Assessment
		E)																		
36	3GPP	TS 33.102					X			X						X	X			
37	ISO/IEC	ISO/IEC 9798								X										
38	ISO/IEC	ISO/IEC 11770								X										
39	ISO/IEC	ISO/IEC 13888								X										
40	ISO/IEC	ISO/IEC 14888								X										
41	ISO/IEC	ISO/IEC 15946-1								X										
42	ISO/IEC	ISO/IEC 18033								X										
43	ISO/IEC	ISO/IEC 19772								X										
44	W3C	XML Encryption														X				
45	W3C	XML Signature														X				
46	W3C	Canonical														X				

ID Number	SDO	Standard ID	2.1 Security Policy	2.2 Organizational Security	2.3 Personnel Security	2.4 Physical and Environmental Security	2.5 System and Services Acquisition	2.6 Configuration Management	2.7 Strategic Planning	2.8 System and Communication Protection	2.9 Information and Document Management	2.10 System Development and Maintenance	2.11 Security Awareness and Training	2.12 Incident Response	2.13 Media Protection	2.14 System and Information Integrity	2.15 Access Control	2.16 Audit and Accountability	2.17 Monitoring & Reviewing Control System Security Policy	2.18 Risk Management and Assessment
		XML																		
47	NERC CSSWG (1)[38]																			
48	NERC CSSWG (2)																			
49	NERC CSSWG (3)																			
50	NERC CSSWG (4)																			
51	NERC CSSWG (5)																			
52	IEEE	C37.231																		
53	NIST	FIPS 198								X										
54	NIST	FIBS 180-2								X										
55	ANSI	ANS X9.52-1998								X										

[38] The number in parentheses for the five NERC CSSWG documents is for reference purposes only – to distinguish the five documents

ID Number	SDO	Standard ID	2.1 Security Policy	2.2 Organizational Security	2.3 Personnel Security	2.4 Physical and Environmental Security	2.5 System and Services Acquisition	2.6 Configuration Management	2.7 Strategic Planning	2.8 System and Communication Protection	2.9 Information and Document Management	2.10 System Development and Maintenance	2.11 Security Awareness and Training	2.12 Incident Response	2.13 Media Protection	2.14 System and Information Integrity	2.15 Access Control	2.16 Audit and Accountability	2.17 Monitoring & Reviewing Control System Security Policy	2.18 Risk Management and Assessment
56	NIST	FIPS 197								X										
57	NIST	FIPS 186-3								X										
58	ANSI	ANSI X9.62								X										
59	PKCS	PKCS #1,#3,#5-#12,#15								X										
60	ANSI	ANSI X9.42								X										
62	IETF	IETF 4120								X							X			
63	ANSI/INCITS	INCITS 359															X			
64	NIST	SP 800-63	X							X							X			
65	OASIS	XACML 2.0									X						X			
66	OASIS	SAML 2.0								X	X					X	X	X		
67	OGC	GeoXACML									X						X			

5.3 LAYER OF SECURITY

This table lists each standard, the applicable OSI layer and any additional notes and comments.

Table 5.3 – Standard and Applicable OSI Layer

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
1	IEC	IEC 62351 -1								
2	IEC	IEC 62351 -2								
3	IEC	IEC 62351 -3				X				
4	IEC	IEC 62351 -4							X	
5	IEC	IEC 62351 -5							X	
6	IEC	IEC 62351 -6							X	
7	IEC	IEC 62351 -7							X	
8	IEC	IEC 62351 -8							X	
9	ANSI	ANSI C12.22							X	Application protocol for transport C12.19 metering table data over networks. C12.22 support AES encryption
10	DHS	DHS	X	X	X	X	X	X	X	
11	IEEE	IEEE 802.11i	X	X						WPA2 is a certification program indicating compliance with the security protocol created by Wi-Fi Alliance to secure wireless computer networks. The WPA2 implements the mandatory elements of IEEE Std 802.11i.
12	IEEE	IEEE 1547.3	X			X			X	
13	IEEE	IEEE 1686								This standard provides security requirements for substation equipment. Requirements addressed

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
										include access control, number of distinct accounts, password construction rules (the standard does not address strong authentication), prevention of password bypass or exposure (e.g., during equipment diagnosis), audit trail, configuration, and other requirements. The standard provides language for use in procurements.
14	IETF	SNMP							X	SNMPv3 is defined by RFC 3411–RFC 3418. SNMPv3 primarily added security and remote configuration enhancements to SNMP. SNMPv3 provides important security features: - Message integrity to ensure that a packet has not been tampered with in transit. - Authentication to verify that the message is from a valid source. - Encryption of packets to prevent snooping by an unauthorized source.
15	ISA IEC	SP99 IEC 62443								ISA SP99 The ISA-SP99 Committee addresses manufacturing and control systems whose compromise could result in any or all of the following situations: - endangerment of public or employee safety - loss of public confidence - violation of regulatory requirements - loss of proprietary or confidential information - economic loss - impact on national security

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
										IEC 62443 Title: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models Abstract: IEC/TS 62443-1-1:2009(E) is a technical specification which defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series. The IEC 62443 series is intended to be the internationalized version of the ISA99 series. Some of the ISA99 series documents, such as the second edition of ISA99.02.01 and ISA99.02.02/IEC 62443-2-1 and -2, are planned to be included in the JTC1 27000 series companion IT standards, with the result that they will eventually carry both 62443-2-nn and 2702n numbers. This may also occur for some of the anticipated ISA99.03.nn and ISA99.04.nn documents, if they are written in a manner that fits the outline requirements of 27000-series companion IT standards.
16	ISO	ISO 27000								ISO/IEC 27000 is part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards. ISO/IEC 27000 provides: - An overview of and introduction to the entire ISO/IEC 27000 family of Information Security

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
										Management Systems (ISMS) standards; and - A glossary or vocabulary of fundamental terms and definitions used throughout the ISO/IEC 27000 family.
17	NERC	CIP 002 thru 009								NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. CIP-002-2 Cyber Security - Critical Cyber Asset Identification CIP-003-2 Cyber Security - Security Management Controls CIP-004-2 Cyber Security - Personnel & Training CIP-005-2 Cyber Security - Electronic Security Perimeter(s) CIP-006-2 Cyber Security - Physical Security of Critical Cyber Assets CIP-007-2 Cyber Security - Systems Security Management CIP-008-2 Cyber Security - Incident Reporting and Response Planning CIP-009-2 Cyber Security - Recovery Plans for Critical Cyber Assets

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
18	NIST	FIPS 140-2	X	X	X	X	X	X	X	This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas including cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.
19	NIST	FIPS 197			X	X	X		X	This standard is for the use of AES encryption, how it should be developed and implemented. This standard does specifically media protection, but for sensitive information protection. The applicable layers were checked where the AES encryption may be applied. This standard is not required by any entity and is used by many governmental agencies.
20	NIST	SP 800-53, Rev 3							X	The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines apply to all

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
										components11 of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems and effective risk management within the federal government.
21	NIST	SP 800-82		X	X	X	X	?	?	SP 800-82 provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. SP 800-82 provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.
22	IEC	IEC 61850-3								
23	UCAIug	UCAIug AMI-SEC								
24	OASIS	WS-Security							X	This specification describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. This specification also provides a general-purpose

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
										mechanism for associating security tokens with message content.
25	IEEE	802.1AR								
26	IEEE	802.1AE								
27	IEEE	802.1X-REV								
28	IETF	TLS								
29	IETF	DTLS								
30	IETF	IPSec								
31	IETF	RFC3711								
32	IETF	RFC4962								
33	IETF	RFC 3748								
34	IEEE	802.16e								
35	NIST	NIST SP 800-38(A-E)								
36	3GPP	TS 33.102		X	X				X	
37	ISO/IEC	ISO/IEC 9798							X	Entity authentication based on cryptographic check function, symmetric encipherment algorithms, and digital signature techniques.
38	ISO/IEC	ISO/IEC 11770							X	ISO/IEC 11770 specifies key management mechanisms based on symmetric, asymmetric and weak secrets.
39	ISO/IEC	ISO/IEC 13888							X	Non repudiation mechanisms provide protocols for the exchange of non-repudiation tokens for non-repudiation services.

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
40	ISO/IEC	ISO/IEC 14888							X	ISO/IEC 14888-1:2008 specifies general principles and requirements for digital signatures with appendix. ISO/IEC 14888-2 addresses digital signatures based on integer factoring, and ISO/IEC 14888-3 addresses digital signatures based on discrete logarithm.
41	ISO/IEC	ISO/IEC 15946-1							X	ECC is an approach to public key cryptography based on elliptic curves. ECDH, ECDSA, and ECMQV are some of the cryptographic schemes based on elliptic curves.
42	ISO/IEC	ISO/IEC 18033							X	ISO/IEC 18033 specifies encryption systems for the purpose of data confidentiality.
43	ISO/IEC	ISO/IEC 19772							X	Authenticated encryption provides CIA guarantees. ISO/IEC 19772:2009 specifies six methods for authenticated encryption.
44	W3C	XML Encryption								Provides encryption of XML documents on either a total document or an individual element basis.
45	W3C	XML Signature								Provides both signature for non-repudiation and integrity check capability for XML documents on either a total document or individual element basis.
46	W3C	Canonical XML								In applying encryption for either confidentiality or integrity to XML documents, the results are dependent on white space, i.e., two documents having the same content will have different results. This standard provides a canonical form of XML intended to provide the same results in all cases.

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
47	NERC CSSWG (1)[39]									"The purpose of this guideline is to provide suggestions for creating and deploying an effective incident response plan for control systems. A well-formed incident response plan will help minimize possible impacts of cyber security incidents and assist in the identification, classification, response, and reporting of cyber security incidents related to critical cyber assets."
48	NERC CSSWG (2)									"The purpose of this guideline is to provide recommendations to effectively and reliably secure control system networks that are electronically connected to business networks. Specifically, this guideline offers recommendations that can decrease the likelihood of a cyber security intrusion on the control system originating from the business network."
49	NERC CSSWG (3)									"The purpose of this guideline is to provide suggestions for an effective cyber security patch management strategy for control systems. "
50	NERC CSSWG (4)									
51	NERC CSSWG									"The purpose of this Guideline is to describe minimum recommendations for maintaining accurate

[39] [39] The number in parentheses for the five NERC CSSWG documents is for reference purposes only – to distinguish the five documents.

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
	(5)									time stamp indications for logged events on the bulk power system."
52	IEEE	C37.231								This recommended practice deals with the implications surrounding the use and administration of firmware revisions for protection-related equipment. In general, the number of firmware revisions has become prolific since the introduction of microprocessor-based protection related equipment and no standard means of dealing with the issues surrounding this situation has been addressed. This recommended practice attempts to provide guidelines for producers, distributors, and users of protection related equipment utilizing firmware with the intent of helping to maximize the security and reliability of the power system.
53	NIST	FIPS 198							X	HMAC is a type of MAC involving a cryptographic hash function and a secret key. HMAC provides both message integrity and message authentication.
54	NIST	FIBS 180-2		X	X	X			X	SHA-256 is the standard that was reviewed. It is a cryptographic hash function used to generate message digests.
55	ANSI	ANS X9.52-1998							X	Triple DES is a block cipher based on DES. It provides a method to extend the key size of DES to protect against brute force attacks.
56	NIST	FIPS 197							X	AES is a block encryption cipher based on substitution permutation network.
57	NIST	FIPS 186-3							X	This Standard specifies a suite of algorithms that can

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
										be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.
58	ANSI	ANSI X9.62							X	The Elliptic Curve Digital Signature Algorithm (ECDSA) is specified in ANS X9.62. FIPS 186-3 approves the use of ECDSA, but specifies additional requirements. Recommended elliptic curves for Federal Government use are provided in FIPS 186-3.
59	PKCS	PKCS #1,#3,#5-#12,#15							X	PKCS is a collection of public key cryptography standards devised by RSA Security.
60	ANSI	ANSI X9.42							X	Diffie-Hellman is a cryptographic protocol allowing two parties to establish a shared secret key over an insecure communication channel.
62	IETF	IETF 4120							X	Kerberos is an authentication protocol providing mutual authentication. Kerberos builds on symmetric key cryptography and requires a trusted third party.
63	ANSI/INCITS	INCITS 359							X	Role based access control is an approach to restricting system access to authorized users. NIST RBAC model describes a standardized definition of

ID Number	SDO	Standard ID	Physical Layer	Data Link Layer	Network Layer	Transport Layer	Session Layer	Presentation Layer	Application Layer	Notes and/or Comments
										role based access control.
64	NIST	SP 800-63								This recommendation provides technical guidance implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions. Although focused on providing guidance to Federal agencies, the information in the document can be adapted to the needs of the Smart Grid and the FERC-mandated inclusion of strong authentication in the CIP requirements for the Bulk Electric System.
65	OASIS	XACML 2.0							X	Provides XML-based security policy language for access control. Includes Core Specification, RBAC Profile, Hierarchical Resource Profile, Multiple Resource Profile, Privacy Policy Profile, SAML 2.0 Profile, and XML Digital Signature Profile
66	OASIS	SAML 2.0							X	SAML provides an XML-based framework for creating and exchanging security information between online partners.
67	OGC	GeoXACML							X	Extends OASIS XACML standard to allow creation of access control policies using geographic data types, functions, and operators.

CHAPTER SIX
RESEARCH AND DEVELOPMENT THEMES FOR CYBER SECURITY IN THE SMART GRID

6.1 INTRODUCTION

Cyber security is one of the key technical areas where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid. This chapter is the deliverable produced by the Research and Development (R&D) subgroup of SGIP-CSWG based on the inputs from various group members. In general, research involves discovery of the basic science that supports a product's viability (or lays the foundation for achieving a target that is currently not achievable), development refers to turning something into a useful product or solution, and engineering refines a product or solution to a cost and scale that makes it economically viable. Another differentiation is basic research which delves into scientific principles (usually done in universities) and applied research which uses basic research to better human lives. Research can be theoretical or experimental. Finally, there are long-term (5-10 yrs) and short-term (less than 5 yrs) research. This chapter stops short of specifying which of the above categories each research problem falls into. That is, we do not discuss whether something is research, development, engineering, short-term or long-term, although we might do so in future revisions. In general, this chapter discusses problems that arise or are expected to arise in the Smart Grid that do not yet have commercially viable solutions.

The topics are partly based on experience of members of the SGIP-CSWG R&D group and research problems that are widely publicized. The raw topics submitted by individual group members were collected in a flat list and iterated over to disambiguate and re-factor them to a consistent set. The available sections were then edited, consolidated and reorganized as the following five high-level theme areas:

1. Device Level
2. Novel Mechanisms
3. Systems Level
4. Networking Issues
5. Other Security Issues in the Smart Grid Context

These five groups collectively represent an initial cut at the thematic issues requiring immediate research and development to make the Smart Grid vision a viable reality. We expect that this R&D group will continue to revise and update this document as new topics are identified from other SGIP-CSWG subgroups such as bottom-up, vulnerability, and privacy; by comments from readers; and by tracking government, academic and industry research efforts that are related to Smart Grid cyber security. These research efforts include the US Department of Energy Control System Security and the National SCADA Testbed programs, US Department of Homeland Security Control System Security program and Cyber Physical Systems Security efforts (see https://www.enstg.com/Signup/files/DHS%20ST%20Cyber%20Workshop%20Final%20Report-v292.pdf), the industry Roadmap to Secure Control Systems, the UCA International Users group focusing on AMI security, and the North American Synchrophasor Initiative.

6.2 DEVICE LEVEL TOPICS

6.2.1 Cost Effective Tamper Resistant Device Architectures

Improve Cost Effective Higher Tamper Resistant and Survivable Device Architectures

As IEDs play more critical roles in the Smart Grid, one needs to ensure that the devices are not easily attacked by firmware updates, commandeered by a spoofed remote device, or swapped out by a rogue device. At the same time, because of the unique nature and scale of these devices, protection measures need to be cost effective (deployment and use) and mass producible. There are some initial forms of these technologies in the field but there is a growing belief that they need to be further improved as security researchers have already demonstrated penetrations of these devices, even with some reasonable protections. Further, it is important to assume devices will become penetrated and there must be a method for their containment and secure recovery using remote means. This is of great importance to maintain the reliability and overall survivability of the Smart Grid. Please see Chapter Three for a discussion of defense-in-depth on a systems basis that would begin to address these issues.

Research is needed in devising scalable, cost-effective device architectures that can form a robust hardware and software basis for overall systems level survivability and resiliency that:

- Are highly tamper resistant and evident, and can provide for secure remote recovery
- Improve security of firmware/software upgrades

Without these R&D advances, local attacks can become distributed/cascading large scale attack campaigns.

Potential starting points are:

- NIST crypto tamper evident requirements;
- Mitigating (limiting) the value of attacks at end points (containment regions in the Smart Grid architecture); and
- Expiring lightweight keys.

6.2.2 Intrusion Detection with Embedded Processors

Research is needed to find ways to deal with the special features and specific limitations of embedded processors used in the power grid. A large number of fairly powerful processors, but with tighter resources than general purpose computers and strict timeliness requirements, embedded in various types of devices are expected to form a distributed inter-network of embedded systems. Intrusion detection in such systems is not merely adapting the types of intrusion detection developed for classical IT systems. Section 6.6.4 discusses this issue in the context of protecting cyber-power systems.

This work would also investigate the possible applications of advanced intrusion detection systems and the types of intrusion detection that may be possible for embedded processors, such as real-time intrusion detection.

6.3 NOVEL MECHANISMS

6.3.1 Topics in Cryptographic Key Management

Smart Grid deployments such as AMI will entail remote control of a large number of small processors acting as remote sensors such as meters. Security for such systems entails both key management on a scale involving possibly tens of millions of credentials and keys, and local cryptographic processing on the sensors such as encryption and digital signatures. This calls for research on large-scale and economic key management in conjunction with cryptography that can be carried out effectively on processors with strict limits on space and computation. This cryptography and key management should ideally be strong and open (free of intellectual property issues) to foster the necessary interoperability standards of the Smart Grid. Existing key management systems and methods could be explored as a basis of further innovation; examples can include PKI (Public Key Infrastructure), IBE (Identity-Based Encryption), hierarchical, decentralized, and delegated schemes and their hybridization.

There are also problems of ownership (e.g., utility vs. customer owned) and trust and how those must be optimally managed in environments where there is little physical protection, and access may happen across different organizational and functional domains (e.g., hub of multiple vendors/service providers, in-home gateway, aggregator, etc.) with their own credentials and security levels. This requires research into new forms of trust management, partitioning, tamper-proofing/detection, and federated ID management that can scale and meet reliability standards needed for the Smart Grid.

On the various devices/systems that will be found in areas of distributed automation, AMI, distributed generation, substations, etc. there are many resource constraining factors that have to do with limited memory, storage, power (battery, or long sleep cycles), bandwidth, and intermittent connections. All of these factors require that research be accomplished into more efficient, adhoc, and flexible key management that require less centralization and persistent connectivity and yet can retain the needed security and trust levels of the entire infrastructure as compared to conventional means.

Emergency (bypass) operations are a critical problem that must optimally be addressed. We cannot afford to have security degrade reliability of the system by having personnel/systems "locked out" during a critical event. Similarly restoring power may require systems to "cold boot" their trust/security with little to no access to external authentication/authorization services. This requires research into key management and cryptography schemes that can support bypass means and yet remain secure in their daily operations.

One has to ensure that encrypted communications do not hinder existing power system and information and communication systems monitoring (possibly from multiple parties of different organizations) for reliability and security requirements. Depending on the system context this problem may require research into uniquely secure and diverse escrow schemes and supporting key management and cryptography that meets the various requirements of the Smart Grid that have been discussed.

6.3.2 Detecting Anomalous Behavior Using Modeling

Various sensors in the power/electrical domain already collect a wide array of data from the grid. In the Smart Grid, there will also be a number of sensors in the cyber domain that will provide

data about the computing elements as well as about the electrical elements. In addition to naturally occurring noise, some of the sensor data may report effects of malicious cyber activity and "misinformation" fed by an adversary.

Reliable operation of the Smart Grid depends on timely and accurate detection of outliers and anomalous events. Power grid operations will need sophisticated outlier detection techniques that enable the collection of high integrity data in the presence of errors in data collection.

Research in this area will explore developing normative models of steady state operation of the grid and probabilistic models of faulty operation of sensors. Smart Grid operators can be misguided by intruders who alter readings systematically, possibly with full knowledge of outlier detection strategies being used. Ways of detecting and coping with errors and faults in the power grid need to be reviewed and studied in a model that includes such systematic malicious manipulation. Research should reveal the limits of existing techniques and provide better understanding of assumptions and new strategies to complement or replace existing ones.

Some example areas where modeling research could lead to development of new sensors:

- Connect/disconnect reporting information from meters may identify an unauthorized disconnect, which, in the context appropriate domain knowledge can be used to determine root cause. This research would develop methods to determine when the number of unauthorized disconnects should be addressed by additional remediation actions to protect the overall AMI communications infrastructure, as well as other distribution operations (DR events, etc.).
- Information about meters running backwards could generally be used for theft detection (for those customers not subscribed to net metering). This research would identify thresholds where too many unauthorized occurrences would initiate contingency operations to protect the distribution grid.

Fraud detection algorithms and models used in credit card transaction monitoring may be relevant to this application.

6.4 Systems Level Topics (Security and Survivability Architecture of the Smart Grid)

While it is not uncommon for modern distribution grids to be built to withstand some level of tampering to meters and other systems that cannot be physically secured, as well as a degree of invalid or falsified data from Home Area Network (HAN) networks, the envisioned Smart Grid will be a ripe target for malicious, well-motivated, well-funded adversaries. The increased dependence on information and distributed and networked information management systems in SCADA, WAMS, and PLCs imply that the Smart Grid will need much more than device authentication, encryption , fail over and models of normal and anomalous behavior, all of which are problems on their own given the scale and timeliness requirement of the Smart Grid. The Smart Grid is a long term and expensive resource, it must be built future-proof—it needs to be built to adapt to changing needs in terms of scale and functionality, and at the same time it needs to be built to tolerate and survive malicious attacks of the future that we cannot even think of at this time. Research is clearly needed to develop an advanced protection architecture that is dynamic (can evolve) and focuses on resiliency (tolerating failures, perhaps of a significant

subset of constituents). A number of research challenges that are particularly important in the Smart Grid context area are described below.

6.4.1 Architecting for bounded recovery and reaction

Effective recovery requires containing the impact of a failure (accidental or malicious); enough resources and data (e.g., state information) positioned to regenerate the lost capability; and real-time decision making and signaling to actuate the reconfiguration and recovery steps. Even then, guaranteeing the recovery within a bounded time is a hard problem, and can only be achieved under certain conditions. To complicate things further, different applications in a Smart Grid will have different elasticity and tolerance, and recovery mechanisms may themselves affect the timeliness of the steady state, not-under attack operation.

With the presence of renewable energy sources that can, under normal operation, turn on or off unpredictably (cloud over or lack of wind) and mobile energy sinks (such as the hybrid vehicle) whose movement cannot be centrally controlled, the Smart Grid becomes much more dynamic in its operational behavior. Reliability will increasingly depend on the ability to react to these events within a bounded time and limiting the impact of changes within a bounded spatial region. How does one architect a wide area distributed system of the scale of the Smart Grid such that its key components and designated events have a bounded recovery and reaction time and space? What resources need to be available, what cryptographic/key material need to be escrowed or made available, how much data needs to be check pointed and placed at what location, what is the circle of influence that one needs to consider to facilitate bounded recovery and reaction--these are the questions that this R&D task should answer.

6.4.2 Architecting Real-time security

In the context of Smart Grid, the power industry will increasingly rely on real time systems for advanced controls. These systems must meet requirements for applications that have a specific window of time to correctly execute. Some “hard real time” applications must execute within a few milliseconds. Wide area protection and control systems will require secure communications that must meet tight time constraints. Cyber physical systems often entail temporal constraints on computations because control must track the dynamic changes in a physical process. Typically such systems have been treated as self-contained and free of cyber security threats. However, increasing openness and interoperability, combined with the threat environment today, requires that such systems incorporate various security measures ranging from device and application authentication, access control, redundancy and fail over for continued operation, encryption for privacy and leakage of sensitive information. Insertion of these mechanisms has the potential to violate the real time requirements by introducing uncontrollable or unbounded delays.

Research in this area should provide strategies for minimizing and making predictable the timing impacts of security protections such as encryption, authentication, and re-keying and exploiting these strategies for grid control with security.

6.4.3 Calibrating assurance and timeliness tradeoffs

There are various sources of delay in the path between two interacting entities in the Smart Grid (e.g., sensor that captures the measurement sample such as the PMUs to the application that consumes it, or from the applications at the control center that invoke operations, uploads firmware or change parameter value on a remote smart device). Some of them are security

mechanisms that already exist in the system. Many of these sources of delays can be manipulated by a malicious adversary. To defend against these, additional security mechanisms are needed, which in turn may add more delay. On the other hand, security is not absolute, and quantifying cyber-security is already a hard problem. Given the circular dependency between security and delay, the various delay sources in the wide area system, and the timeliness requirements of the Smart Grid applications, there is a need and challenge to organize and understand the delay-assurance trade space for potential solutions that are appropriate for the grid applications. Without this understanding, at times of crisis, operators will be ill-prepared, and will have to depend on individual's intuition and expertise. On the other hand, if the tradeoffs are well understood, it will be possible to develop and validate contingencies that can be quickly invoked or offered to human operators at times of crisis

6.4.4 Legacy system integration

Integrating with legacy systems is a hard and inescapable reality in any realistic implementation of Smart Grid. This poses a number of challenges to the security architecture of the Smart Grid:

- Compatibility problem with new security solutions installed in new device: mismatched expectation may cause the devices to fail or malfunction (anecdotal story of a network scan using tools like NMAP tripping of IEDs because they do not implement the TCP/IP stack fully) and
- Backwards compatibility: often this may be a requirement (regulator, owner organization) and may prevent deployment of advanced features.

Relevant effort:

- Not just link encryptors, but research in legacy systems, beyond SCADA encryption, AGA12 (American Gas Association) Archives.

Potential avenues of investigation include:

- 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 architecture design, possibly using red team methodology.

6.4.5 Resiliency Management and Decision Support

This research will look at threat response escalation as a method to maintain system resiliency. While other Smart Grid efforts are targeted at improving the security of devices, this research focuses on the people, processes and technology options available to detect and respond to threats that have breached those defenses in the context of the Smart Grid's advanced protection architecture. Some of the responses must be autonomic—timely response is a critical requirement for grid reliability. However, for a quick response to treat the symptom locally and effectively, the scope and extent of the impact of the failure needs to be quickly determined. Not all responses are autonomic however. New research is needed to measure and identify the scope of a cyber attack and the dynamic cyber threat response options available in a way that can serve as a decision support tool for the human operators.

6.4.6 Efficient Composition of Mechanisms

It can sometimes be the case that even though individual components work well in their domains, compositions of them can fail to deliver the desired combination of attributes, or fail to deliver them efficiently. For example, a protocol in the X.509 draft standard was found to have a flaw which allowed an old session key to be accepted as new. Formal methods for cryptographic algorithm composition have helped, but tend to concentrate on small, specific models of individual protocols rather than the composition of multiple algorithms as is typically the case in real implementations. In other circumstances, the composition of two useful models can cause unintended and unwanted inefficiencies. An example of this is the combination of the congestion control of TCP overlaid over ad-hoc mobile radio networks.

Research which systematizes the composition of communications and/or cryptographic mechanisms and which assists practitioners in avoiding performance, security or efficiency pitfalls would greatly aid the creation and enhancement of the Smart Grid.

6.4.7 Risk Assessment and Management

A risk-based approach is a potential way to develop viable solution to security threats and measure the effectiveness of those solutions. Applying risk based approaches to cyber security in the Smart Grid context raises a number of research challenges. The following are three important ones.

Advanced Attack Analysis

While it is clear that cyber attacks or combined cyber/physical attacks pose a significant threat to the power grid, advanced tools and methodologies are needed to provide a deep analysis of cyber and cyber/physical attack vectors and consequences on the power grid. For example, answering questions such as, “can a cyber or combined cyber/physical attack lead to a blackout?”

Measuring Risk

The state of the art in this area is limited to surveys and informal analysis of critical assets and the impact of their compromise or loss of availability. Advanced tools and techniques that provide quantitative notions of risks, that is, threats, vulnerabilities and attack consequences for current and emerging power grid systems will allow for better protection and regulation of power systems.

Risk-based Cyber Security Investment

When cyber security solutions are deployed they mitigate risks. However, it is hard to assess the extent to which risk has been mitigated. A related question is how much investment in cyber security is appropriate for a given entity in the electric sector? Research into advanced tools and technologies based on quantitative risk notions can provide deeper insights to answer this question.

6.5 NETWORKING TOPICS

6.5.1 Safe use of COTS/Publicly Available Systems and Networks

Economic and other drivers push the use of COTS (commercial-off-the-shelf) components, public networks like the Internet or the sharing of available Enterprise systems. Research is needed to investigate the extent such resources can be used in the Smart Grid reliably and safely.

Use of the Internet in Smart Grid: A specific case is the use of the existing Internet in Smart Grid related communications, including possibly as an emergency out-of-band access infrastructure. The Internet is readily available, evolving and inherently fault tolerant. But it is also shared, contains numerous malicious malware and malicious activities. Methods to deal with denial of service as well as identifying other critical issues will serve to understand the strengths and weaknesses as well as cautions of using the existing Internet for specific types of Smart Grid applications.

Security/reliability issues surrounding the adaption of TCP/IP is a related research topic that investigates security topics related to the adoption of the Internet Protocols for Smart Grid networks. This is a separate topic from Internet use. Research could include understanding the current state of security designs proposed for advanced networks. Features such as Quality of Service, Mobility, Multihoming, Broadcasting/Multicasting and other enhancements necessary for Smart Grid applications must be adequately secured and well managed if it is to be adopted.

6.5.2 Advanced Networking

The prevalent notion is that Smart Grid communications will be primarily TCP/IP based. Advanced networking technologies independent of the Internet Protocols are being explored in multiple venues under the auspices of NSF, DARPA and others. Advanced networking development promises simpler approaches to networking infrastructure that solve by design some of the issues now facing the Internet Protocols. The work however is not complete but should be understood in the context of providing secure networks with fewer complexities and can be more easily managed and offer more predictable behavior.

A wide variety of communication medium is currently available and being used today ranging from leased lines, microwave links, wireless, power line communication etc. Any advanced networking technology that aims to provide a uniform abstraction for Smart Grid communication must also needs to support these various physical layers.

6.6 OTHER SECURITY ISSUES IN THE SMART GRID CONTEXT

If the Smart Grid is viewed as a cyber-physical system, then the cyber cross-section of the Smart Grid will look like a large federated distributed environment where information systems from various organizations with very different characteristics and purpose will need to interoperate. Among the various interacting entities are utilities, power generators, regulating authorities, research and institutions, even large industrial consumers (if the likes of Google are allowed to buy electricity directly) and with the advent of home based renewable and hybrid vehicles, possibly residential customers. Effectively securing the interfaces between environments will become an increasing challenge as users seek to extend Smart Grid capabilities. Scalable and secure inter-organizational interaction is a key security and management issue. Privacy policies involving data in at rest, in transit, and in use will have to be enforced within and across these environments. Research is needed in the following areas.

6.6.1 Privacy and Access Control in Federated Systems

1. **Managed separation of business entities**: Research in this area will focus on the network and systems architecture that enables effective communication among the various business entities without inadvertent sharing/leakage of their trade secrets, business strategies or operational data and activities. It is anticipated fine-grained energy data and various other types of information will be collected (or will be available as a byproduct of interoperability) from businesses and residences to realize some of the advantages of Smart Grid technology.
    a. Techniques to specify and enforce the appropriate sharing policies among entities with various cooperative, competing, regulatory relationships are not well understood today. Work in this area would mitigate these risks and promote confidence among the participants that they are not being illegitimately monitored by their energy service provider, regulatory bodies or competitors. Architectural solutions will be important for this objective, but there are also possibilities for improvements, for example, privacy enhancing technologies based on cryptography or work on anonymity protections.
    b. As they collect more information, energy service providers will need to manage large amounts of privacy-sensitive data in an efficient and responsible manner. Research on privacy policy and new storage management techniques will help to diminish risk and enhance the business value of the data collected while respecting customer concerns and regulatory requirements. Such work would contribute to improved tracking of the purpose for which data was collected and enable greater consumer discretionary control.
    c. Verifiable enforcement of privacy policies regardless of the current state and location of data will provide implicit or explicit trust in the Smart Grid. Research is needed to develop policies and mechanisms for such enforcement.
2. **Authentication and Access Control in a highly dynamic federated environment:** Collaborating autonomous systems in a federated environment must need to invoke operations on each other, other than accessing collected data (e.g., an ISO asking for more power from a plant)-- access control (authentication and authorization), and especially when the federates enter in dynamic relationships (daily buy/sell, long term contracts etc) is an issue that needs research as well.

6.6.2 Auditing and Accountability

The concept of operation of the envisioned smart grid will require collecting audit data from various computer systems used in the Smart Grid. The existence of multiple autonomous federated entities makes this problem even more complex: who is responsible for auditing whom, how to link the audit trails collected at various points, what mechanism can be used to mine the data thus collected etc. Such data will be needed to assess status, including evidence of intrusions and insider threats. Research is needed on a range of purposes for which audit data will be needed and on finding the best ways to assure accountability for operator action in the system. This will include research on forensic techniques to support tracing and prosecution of attackers and evidence to regulatory agencies without interruption of operations.

6.6.3 Infrastructure Interdependency Issues

Maintaining the resiliency and continuous availability of the power grid itself as a critical national infrastructure is an important mandate. There are also other such critical national infrastructure elements as well, such as telecommunications, oil and natural gas pipelines, water distribution systems, etc. with as strong a mandate for resiliency and continuous availability. However, the unique nature of the electrical grid is that it supplies key elements toward the well being of these other critical infrastructure elements. And additionally, there are reverse dependencies emerging on Smart Grid being dependent on the continuous well being of the telecommunications and digital computing infrastructure, as well as on the continuing flow of the raw materials to generate the power. These interdependencies are sometimes highly visible and obvious, but many remain hidden below the surface of the detailed review for each. There is little current understanding of the cascading effect outages and service interruptions might have, especially those of a malicious and judiciously placed nature with intent to cause maximum disruption and mass chaos. This research would investigate and identify these dependencies, and work on key concepts and plans toward mitigating them, from the perspective of the Smart Grid. It should lead to techniques that show not only how communication failures could impact grid efficiency and reliability, how power failures could affect digital communications, and how a simultaneous combination of failures in each of the systems might impact the system as a whole, but also apply a rigorous approach to identifying and highlighting these key interdependencies across all of these critical common infrastructure elements. The research would need to develop and apply new system of systems concepts and design approaches toward mitigating these interdependencies at nationwide scale.

6.6.4 Cross-Domain (Power/Electrical to Cyber/Digital) Security Event Detection, Analysis, and Response

The implication of failures or malicious activity in the cyber domain on the electrical domain, or vice versa, in the context of a large-scale and highly dynamic distributed cyber-physical system such as the Smart Grid is not well understood. Without further research, this is going to remain a dark area, which carries a big risk for the operational reliability and resiliency of the power grid.

As mentioned throughout various sections of this document there is a need to better integrate the cyber and power system view, This is especially important in regards to detecting security events such as intrusions, unauthorized accesses, mis-configurations, etc., as well as anticipating cyber and power system impacts and forming a correct and systematic response on this basis. This is driven by the goal of using the modern IT and communications technologies in the Smart Grid to enhance the reliability of the power system and not offer a risk of degrading it. This will require research into new types of risk and security models as well as methods and technologies.

There is a need to further research and develop models, methods, and technologies in the following example areas:

- Unified risk models that have a correlated view of cyber and power system reliability impacts
- Response and containment models/strategies that use the above unified risk models.
- Security and reliability event detection models that use power and IT and communication system factors in a cross correlated manner and can operate on an autonomous, highly scaled, and distributed basis (e.g., security event detection in mesh networks with

resource constrained devices, distributed and autonomous systems with periodic connectivity, or legacy component systems with closed protocols).

- Unified intrusion detection/prevention systems that use the models/methods above and have a deep contextual understanding of the Smart Grid and its various power system and operations interdependencies.
- Very large scale wide area security event detection and response systems for the Smart Grid that can interoperate and securely share event data across organizational boundaries and allow for intelligent, systematic, and coordinated responses on a real-time or near real-time basis.
- Advanced Smart Grid integrated security and reliability analytics that provide for event and impact prediction and continual infrastructure resiliency improvement.

In order to develop and refine the modeling and systems necessary for much of this proposed research there would also be a need for developing new simulation capabilities of the distribution grid that incorporate communications with devices/models for distribution control, distributed generation, storage, PHEV, etc. to provide a representative environment to evaluate the impact of various events. To provide a realistic assessment of impact, the simulation capabilities should be similar in fidelity to the transmission grid simulation capabilities that currently exist. However both the distribution and transmission grid system simulations need to be further developed to integrate cyber elements and their possible cross impacts on each other.

APPENDIX A
KEY POWER SYSTEM USE CASES FOR SECURITY REQUIREMENTS

The focus of this appendix, "Key Power System Use Cases and Security Requirements" is to identify the key Use Cases that are "architecturally significant" and is neither exhaustive nor complete. New Use Cases may be added to this section in future versions of this document as they become available. This selection of Use Cases will be used for evaluating smart grid characteristics and their associated cyber security objectives, high-level requirements (Integrity, Availability, and Confidentiality) and stakeholder concerns. In addition, the focus is more on operational functions as opposed to "back office" or corporate functions, since it is the automation and control aspects of power system management that are relatively unique and certainly are the ones that stretch the security risk assessment, the security controls, and the security management.
There are many interfaces and "environments" with constraints and sensitive aspects that make up the information infrastructure which is monitoring and controlling the power system infrastructure. This document does not directly capture those distinctions, but leaves it up to the implementers of security measures to take those into account. The Use Cases were derived "as-is" and put into a common format for evaluation. This is not a listing of recommended or mandatory Use Cases, and is not intended for architecting systems or identifying all the potential scenarios that may exist. The full sets of Use Cases, taken from many sources, include the following:

- **IntelliGrid Use Cases** (IntelliGrid web site: http://intelligrid.ipower.com/IntelliGrid_Architecture/Use_Cases/Fun_Use_Cases.htm). There are over 700 of these Use Cases, but really only the power system operations Use Cases and Demand Response/AMI ones are of particular interest for security. The EPRI IntelliGrid project developed the complete list of Use Cases.

- **AMI Business Functions** which were extracted from Appendix B of the AMI-SEC Security Requirements Specification (T&D DEWG and now also posted on SGIP-CSWG TWiki).
- **Benefits and Challenges of Distribution Automation** – Use Case Scenarios (White Paper for Distribution on T&D DEWG, extracted from CEC document which has 82 Use Cases, and now also posted on SGIP-CSWG TWiki).

- **EPRI Use Case Repository** (http://www.smartgrid.epri.com/usecaserepository.html) which is a compilation of IntelliGrid and SCE Use Cases, plus others.

- **SCE Use Cases** (http://www.sce.com/usecases) These were developed by Southern California Edison (SCE) with the assistance of EnerNex.

There is a certain amount of overlap in these sources, particularly in the new area of AMI, but no-one would argue that even the combined set (reaching over 1000 Use Cases) really covers all requirements - they just act as indications of the areas of interactions. For instance, for just one item, the connect/disconnect of meters, 6 utilities developed over 20 Use Case variations in order to meet their diverse needs, often due to different State regulatory requirements.

The Use Cases were not generally copied verbatim from their sources, but sometimes edited to focus on the security issues.

IAC (Integrity, Availability, Confidentiality) Security Requirements

The following Use Cases can be considered to have key security requirements that may vary in vulnerabilities and impacts, depending upon the actual systems, but that nonetheless can be generally assessed as having security requirements with respect to Integrity, Availability, and Confidentiality (IAC).

Integrity is generally considered the most critical security requirement for power system operations, and includes assurance that:

- Data has not been modified without authorization
- Source of data is authenticated
- Timestamp associated with the data is known and authenticated
- Quality of data is known and authenticated

Availability is generally considered the next most critical security requirement, although the time latency associated with availability can vary:

- 4 ms for protective relaying
- Sub-seconds for transmission wide-area situational awareness monitoring
- Seconds for substation and feeder SCADA data
- Minutes for monitoring non-critical equipment and some market pricing information
- Hours for meter reading and longer term market pricing information
- Days/weeks/months for collecting long term data such as power quality information

Confidentiality is generally the least critical for actual power system operations, although this is changing for some parts of the power system, as customer information is more easily available in cyber form:

- Privacy of customer information is the most important
- Electric market information has some confidential portions
- General corporate information, such as human resources, internal decision-making, etc.

Critical Issues for the Security Requirements of Power Systems

The automation and control systems for power system operations have many differences from most business or corporate systems. Some particularly critical issues related to security requirements include:

- Operation of the power system must continue 24x7 with high availability (e.g. 99.99% for SCADA and higher for protective relaying) regardless of any compromise in security or the implementation of security measures which hinder normal or emergency power system operations.
- Power system operations must be able to continue during any security attack or compromise (as much as possible).
- Power system operations must recover quickly after a security attack or compromised information system.
- The complex and many-fold interfaces and interactions across this largest machine of the world – the power system – makes security particularly difficult since it is not easy to separate the automation and control systems into distinct “security domains”. And yet end-to-end security is critical.

- There is not a one-size-fits-all set of security practices for any particular system or for any particular power system environment.
- Testing of security measures cannot be allowed to impact power system operations.
- Balance is needed between security measures and power system operational requirements. Absolute security is never perfectly achievable, so the costs and impacts on functionality of implementing security measures must be weighed against the possible impacts from security breaches.
- Balance is also needed between risk and the cost of implementing the security measures.

Security Programs and Management

Development of security programs is critical to all Use Cases, including:

- Risk Assessment to develop security requirements based on business rational (e.g. impacts from security breaches of IAC) and system vulnerabilities.
    - The likelihood of particular threat agents, which are usually included in risk assessments, should only play a minor role in the overall risk assessment since the power system is so large and interconnected that appreciating the risk of these threat agents would be very difficult.
    - However, in detailed risk assessments of specific assets and systems, some appreciation of threat agent probabilities is necessary to ensure that an appropriate balance between security and operability is maintained.
- Security technologies that are needed to meet the security requirements:
    - Plan the system designs and technologies to embed the security from the start
    - Implement the security protocols
    - Add physical security measures
    - Implement the security monitoring and alarming tools
    - Establish Role-Based Access Control to authorize and authenticate users, both human and cyber, for all activities, including password/access management, certificate and key management, and revocation management
    - Provide the security applications for managing the security measures
- Security policies, training, and enforcement to focus on the human side of security, including:
    - Normal operations
    - Emergency operations when faced with a possible or actual security attack
    - Recovery procedures after an attack
    - Documentation of all anomalies for later analysis and re-risk assessment.
- Conformance testing for both humans and systems to verify they are using the security measures and tools appropriately and not by-passing them:
    - Care must be taken not to impact operations during such testing
    - If certain security measures actually impact power system operations, the balance between that impact and the impact of a security compromise should be evaluated
- Periodic re-assessment of security risks

Category: AMI		
Scenario: Meter Reading Services		
Category Description AMI systems consist of the hardware, software and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third party systems which are interfaced to the AMI systems.		
Scenario Description Meter reading services provide the basic meter reading capabilities for generating customer bills. Different types of metering services are usually provided, depending upon the type of customer (residential, smaller commercial, larger commercial, smaller industrial, larger industrial) and upon the applicable customer tariff. Periodic Meter Reading On-Demand Meter Reading Net Metering for DER and PEV Feed-In Tariff Metering for DER and PEV Bill - Paycheck Matching		
Smart Grid Characteristics Enables active participation by consumers Enables new products, services and markets Optimizes asset utilization and operate efficiently	Cyber Security Objectives/Requirements Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database, to avoid serious breaches of privacy and potential legal repercussions Integrity of meter data is important, but the impact of incorrect data is not large Availability of meter data is not critical in real-time	Potential Stakeholder Issues Customer data privacy and security Retail Electric Supplier access Customer data access

Category: AMI
Scenario: Pre-Paid Metering

Category Description

AMI systems consist of the hardware, software and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third party systems which are interfaced to the AMI systems.

Scenario Description

Customers who either want a lower rate or have a history of slow payment can benefit from prepayment of power. Smart metering makes it easier to deploy new types of prepayment to customers and provide them with better visibility on the remaining hours of power, as well as extending time of use rates to prepayment customers.
AMI systems can also trigger notifications when the pre-payment limits are close to being reached and/or have been exceeded.
Limited Energy Usage
Limited Demand

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Enables new products, services and markets Optimizes asset utilization and operate efficiently	Integrity of meter data is critical, to avoid unwarranted disconnections due to perceived lack of pre-payment. Security compromises could have a large impact on the customer and could cause legal repercussions Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database Availability to turn meter back on after payment is important, but could be handled by a truck roll if necessary	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: AMI

Scenario: Revenue Protection

Category Description

AMI systems consist of the hardware, software and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third party systems which are interfaced to the AMI systems.

Scenario Description

Non-technical losses (or theft of power by another name) has long been an on-going battle between utilities and certain customers. In a traditional meter, when the meter reader arrives, they can look for visual signs of tampering, such as broken seals and meters plugged in upside down. When AMI systems are used, tampering that is not visually obvious may be detected during the analysis of the data, such as anomalous low usage. AMI will help with more timely and sensitive detection of power theft.
Tamper Detection
Anomalous Readings
Meter Status
Suspicious Meter

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Integrity of meter data is important, but if tampering is not detected or if unwarranted indications of tampering are detected, there is no power system impact, just revenue impact Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database Availability to turn meter back on after payment is important	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: AMI

Scenario: Remote Connect/Disconnect of Meter

Category Description

AMI systems consist of the hardware, software and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and

third party systems which are interfaced to the AMI systems.		
Scenario Description Traditionally, utilities send a metering service person to connect or disconnect the meter. With an AMI system, the connect/disconnect can be performed remotely by switching the remote connect/disconnect (RCD) switch for the following reasons. Remote Connect for Move-In Remote Connect for Reinstatement on Payment Remote Disconnect for Move-Out Remote Disconnect for Non-Payment Remote Disconnect for Emergency Load Control Unsolicited Connect / Disconnect Event		
Smart Grid Characteristics Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Cyber Security Objectives/Requirements Integrity of control commands to the RCD switch is critical to avoid unwarranted disconnections or dangerous/unsafe connections. The impact of invalid switching could be very large if many meters are involved Availability to turn meter back on when needed is important Confidentiality requirements of the RCD command is generally not very important, except related to non-payment	Potential Stakeholder Issues Customer data privacy and security Retail Electric Supplier access Customer data access Customer Safety
Category: AMI		
Scenario: Outage Detection and Restoration		
Category Description AMI systems consist of the hardware, software and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third party systems which are interfaced to the AMI systems.		
Scenario Description		

The AMI system detects customer outages and reports it in near-real-time to the distribution utility. The utility uses the customer information from the Customer Information System, the Trouble Call System, Geographical Information System, and the Outage Management System to identify the probable location of the fault. The process includes the following steps:
Smart meters report one or more power losses (e.g. "last gasp")
Outage management system collects meter outage reports and customer trouble calls
Outage management system determines location of outage and generates outage trouble tickets
Work management system schedules work crews to resolve outage
Interactive utility-customer systems inform the customers about the progress of events
Trouble tickets are used for statistical analysis of outages

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Integrity is important to ensure outages are reported correctly Availability is important to ensure outages are reported in a timely manner (a few seconds) Confidentiality is not very important	Customer data privacy and security Retail Electric Supplier access Customer data access Customer Safety

Category: AMI

Scenario: Meter Maintenance

Category Description

AMI systems consist of the hardware, software and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third party systems which are interfaced to the AMI systems.

Scenario Description

Meter maintenance is needed to locate and repair/replace meters that have problems, or to update firmware and parameters if updates are required. For those with batteries, such as gas and water meters, battery management will also be needed.
Connectivity validation
Geo-location of meter

Smart meter battery management		
Smart Grid Characteristics Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Cyber Security Objectives/Requirements Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions Availability is important, but only in terms of hours or maybe days Confidentiality is not important unless some maintenance activity involves personal information	Potential Stakeholder Issues Customer data privacy and security Retail Electric Supplier access Customer data access
Category: AMI		
Scenario: Meter Detects Removal		
Category Description The AMI category covers the fundamental functions of an advanced metering system. These functions include: meter reading, use of an integrated service switch, theft detection and improved outage detection and restoration. The high level technical requirements for these functions are well understood by the industry, but the specific benefit varies from utility to utility. Advanced functions that are often associated with AMI are demand response program support and communications to in-home devices. These functions are not exclusive to AMI and will be discussed in separate category areas.		
Scenario Description This scenario discusses the AMI meter's functionality to detect and report unauthorized removal and similar physical tampering. AMI meters require additional capability over traditional meters to prevent theft and tampering due to the elimination of regular visual inspection provided by meter reading.		
Smart Grid Characteristics Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Objectives/Requirements To reduce energy theft To prevent theft/compromise of passwords and key material To prevent installation of malware	Potential Stakeholder Issues Customer data privacy and security Retail Electric Supplier access Customer data access

Category: AMI		
Scenario: Utility Detects Probable Meter Bypass		
Category Description The AMI category covers the fundamental functions of an advanced metering system. These functions include: meter reading, use of an integrated service switch, theft detection and improved outage detection and restoration. The high level technical requirements for these functions are well understood by the industry, but the specific benefit varies from utility to utility. Advanced functions that are often associated with AMI are demand response program support and communications to in-home devices. These functions are not exclusive to AMI and will be discussed in separate category areas.		
Scenario Description AMI meters eliminate the possibility of some forms of theft (i.e. meter reversal). Other types of theft will be more difficult to detect due to the elimination of regular physical inspection provided by meter reading. This scenario discusses the analysis of meter data to discover potential theft occurrences.		
Smart Grid Characteristics Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Objectives/Requirements To reduce theft To protect integrity of reporting To maintain availability for reporting and billing	Potential Stakeholder Issues Customer data privacy and security Retail Electric Supplier access Customer data access Customer Safety

Category: Demand Response
Scenario: Real Time Pricing (RTP) for Customer Load and DER/PEV
Category Description Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time-based or may be tariff-based, while the prices may also be operationally-based or fixed or some combination. Real-time pricing

inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

Use of Real Time Pricing for electricity is common for very large customers, affording them an ability to determine when to use power and minimize the costs of energy for their business. The extension of real time pricing to smaller industrial and commercial customers and even residential customers is possible with smart metering and in-home displays. Aggregators or customer energy management systems must be used for these smaller consumers due to the complexity and 24x7 nature of managing power consumption. Pricing signals may be sent via an AMI system, the Internet, or other data channels.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Integrity, including non-repudiation, of pricing information is critical, since there could be large financial and possibly legal implications Availability, including non-repudiation, for pricing signals is critical because of the large financial and possibly legal implications Confidentiality is important mostly for the responses that any customer might make to the pricing signals	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: Demand Response

Scenario: Time of Use (TOU) Pricing

Category Description

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time-based or may be tariff-based, while the prices may also be operationally-based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

Time of use pricing creates blocks of time and seasonal differences that allow smaller customers with less time to manage power consumption to gain some of the benefits of real time pricing. This is the favored regulatory method in most of the world for dealing with global warming.
Although Real Time Pricing is more flexible than Time of Use, it is likely that TOU will still provide many customers will all of the benefits that they can profitably use or manage.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Integrity is not critical since TOU pricing is fixed for long periods and is not generally transmitted electronically Availability is not an issue Confidentiality is not an issue, except with respect to meter reading	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: Demand Response

Scenario: Net Metering for DER and PEV

Category Description

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time-based or may be tariff-based, while the prices may also be operationally-based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

When customers have the ability to generate or store power as well as consume power, net metering is installed to measure not only the flow of power in each direction, but also when the net power flows occurred. Often Time of Use (TOU) tariffs are employed.
Today larger C&I customers and an increasing number of residential and smaller C&I customers have net metering installed for their photovoltaic systems, wind turbines, combined heat and power (CHP), and other DER devices. As plug-in electric vehicles (PEVs) become available, net metering will increasingly be implemented in homes and small businesses, even parking lots.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Integrity is not very critical since net metering pricing is fixed for long periods and is not generally transmitted electronically Availability is not an issue Confidentiality is not an issue, except with respect to meter reading	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: Demand Response

Scenario: Feed-In Tariff Pricing for DER and PEV

Category Description

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time-based or may be tariff-based, while the prices may also be operationally-based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

Feed-in tariff pricing is similar to net metering except that generation from customer DER/PEV has a different tariff rate than the customer load tariff rate during specific time periods.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
Enables active participation by consumers Accommodates all generation and storage options Enables new products,	Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically Availability is not an issue Confidentiality is not an issue, except with respect to meter reading	Customer data privacy and security Retail Electric Supplier access Customer data access

services and markets		
Category: Demand Response		
Scenario: Critical Peak Pricing		
Category Description Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time-based or may be tariff-based, while the prices may also be operationally-based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.		
Scenario Description Critical Peak Pricing builds on Time of Use Pricing by selecting a small number of days each year where the electric delivery system will be heavily stressed and increasing the peak (and sometime shoulder peak) prices by up to 10 times the normal peak price. This is intended to reduce the stress on the system during these days.		
Smart Grid Characteristics Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	**Cyber Security Objectives/Requirements** Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically Availability is not an issue Confidentiality is not an issue, except with respect to meter reading	**Potential Stakeholder Issues** Customer data privacy and security Retail Electric Supplier access Customer data access
Category: Demand Response		
Scenario: Mobile Plug-In Electric Vehicle (PEV) Functions		
Category Description Demand response is a general capability that could be implemented in many different ways. The		

primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time-based or may be tariff-based, while the prices may also be operationally-based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

In addition to customers with PEVs participating in their home-based Demand Response functions, they will have additional requirements for managing the charging and discharging of their mobile PEVs in other locations:
Customer connects PEV at another home
Customer connects PEV outside home territory
Customer connects PEV at public location
Customer charges the PEV

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically Availability is not an issue Confidentiality is not an issue, except with respect to meter reading	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: Customer Interfaces

Scenario: Customer's In Home Device is Provisioned to Communicate With the Utility

Category Description

Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in home displays, computers and mobile devices). In addition to real time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.

Scenario Description

This scenario describes the process to configure a customer's device to receive and send data to utility systems. The device could be an information display, communicating thermostat, load control device or smart appliance.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	To protect passwords To protect key material To authenticate with other devices on the AMI system	Customer device standards Customer data privacy and security

Category: Customer Interfaces

Scenario: Customer Views Pricing or Energy Data on Their In Home Device

Category Description

Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in home displays, computers and mobile devices). In addition to real time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.

Scenario Description

This scenario describes the information that should be available to customers on their in home devices. Multiple communication paths and device functions will be considered.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	To validate that information is trustworthy (integrity)	Customer device standards Customer data privacy and security

Category: Customer Interfaces

Scenario: In Home Device Troubleshooting

Category Description

Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in home displays, computers and mobile devices). In addition to real time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.

Scenario Description

This alternate scenario describes the resolution of communication or other types of errors that could occur with in home devices. Roles of the customer, device vendor and utility will be discussed.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	To avoid disclosing customer information To avoid disclosing key material and/or passwords	Customer device standards Customer data privacy and security

Category: Customer Interfaces

Scenario: Customer Views Pricing or Energy Data via the Internet

Category Description

Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in home displays, computers and mobile devices). In addition to real time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.

Scenario Description

In addition to a utility operated communications network (i.e. AMI), the internet can be used to communicate to customers and their devices. Personal computers and mobile devices may be more suitable for displaying some types of energy data than low cost specialized in home display devices. This scenario describes the information that should be available to the customer using the internet and

some possible uses for the data.

Smart Grid Characteristics	**Objectives/Requirements**	**Potential Stakeholder Issues**
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	To protect customer's information (privacy) To provide accurate information	Customer device standards Customer data privacy and security

Category: Customer Interfaces

Scenario: Utility Notifies Customers of Outage

Category Description

Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in home displays, computers and mobile devices). In addition to real time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.

Scenario Description

When an outage occurs the utility can notify affected customers and provide estimated restoration times and report when power has been restored. Smart grid technologies can improve the utility's accuracy for determination of affected area and restoration progress.

Smart Grid Characteristics	**Objectives/Requirements**	**Potential Stakeholder Issues**
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	To validate that the notification is legitimate Customer's information is kept private	Customer device standards Customer data privacy and security

Category: Customer Interfaces

Scenario: Customer Access to Energy-Related Information

Category Description

Customers with Home Area Networks and/or Building Energy Management Systems will be able to interact with the electric utilities as well as third party energy services providers to access information on their own energy profiles, usage, pricing, etc.

Scenario Description

Customers with Home Area Networks and/or Building Energy Management Systems will be able to interact with the electric utilities as well as third party energy services providers. Some of these interactions include:
Access to real-time (or near real-time) energy and demand usage and billing information
Requesting energy services such as move-in/move-out requests, pre-paying for electricity, changing energy plans (if such tariffs become available), etc.
Access to energy pricing information
Access to their own DER generation/storage status
Access to their own PEV charging/discharging status
Establishing thermostat settings for demand response pricing levels
Although different types of energy-related information access is involved, the security requirements are similar.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Integrity, including non-repudiation, is critical since energy and pricing data will have financial impacts Availability is important to the individual customer, but will not have wide-spread impacts Confidentiality is critical because of customer privacy issues	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: Electricity Market

Scenario: Bulk Power Electricity Market

Category Description

The electricity market varies significantly from State to State, region to region, and at local levels. The market is still evolving after some initial setbacks, and is expected to expand from bulk power to retail

power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in a separate section, is a part of the electricity market.

Scenario Description

The bulk power market varies from region to region, and is conducted primarily through Regional Transmission Operators (RTO) and Independent System Operators (ISO). The market is handled independently from actual operations, although the bids into the market obviously affect which generators are used for what time periods and which functions (base load, regulation, reserve, etc.). Therefore there are no direct operational security impacts, but there are definitely financial security impacts.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Integrity for pricing and generation information is critical Availability for pricing and generation information is important within minutes to hours Confidentiality for pricing and generation information is critical	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: Electricity Market

Scenario: Retail Power Electricity Market

Category Description

The electricity market varies significantly from State to State, region to region, and at local levels. The market is still evolving after some initial setbacks, and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in a separate section, is a part of the electricity market.

Scenario Description

The retail power electricity market is still minor, but growing, compared to the bulk power market, but typically involves aggregators and energy service providers bidding customer-owned generation or load control into both energy and ancillary services. Again it is handled independently from actual power system operations. Therefore there are no direct operational security impacts, but there are definitely financial security impacts. (The aggregator's management of the customer-owned generation and load

is addressed in the Demand Response section.)		
Smart Grid Characteristics Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	**Cyber Security Objectives/Requirements** Integrity for pricing and generation information is critical Availability for pricing and generation information is important within minutes to hours Confidentiality for pricing and generation information is critical	**Potential Stakeholder Issues** Customer data privacy and security Retail Electric Supplier access Customer data access
Category: Electricity Market		
Scenario: Carbon Trading Market		
Category Description The electricity market varies significantly from State to State, region to region, and at local levels. The market is still evolving after some initial setbacks, and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in a separate section, is a part of the electricity market.		
Scenario Description The carbon trading market does not exist yet, but the security requirements will probably be similar to the retail electricity market.		
Smart Grid Characteristics Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	**Cyber Security Objectives/Requirements** Integrity for pricing and generation information is critical Availability for pricing and generation information is important within minutes to hours Confidentiality for pricing and generation information is critical	**Potential Stakeholder Issues** Customer data privacy and security Retail Electric Supplier access Customer data access

Category: Distribution Automation

Scenario: Distribution Automation (DA) within Substations

Category Description

A broad definition of Distribution Automation includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/var control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.
Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Distribution automation within substations involves monitoring and controlling equipment in distribution substations to enhance power system reliability and efficiency. Different types of equipment are monitored and controlled:
Distribution SCADA System Monitors Distribution Equipment in Substations
Supervisory Control on Substation Distribution Equipment
Substation Protection Equipment Performs System Protection Actions
Reclosers in Substations

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality for the range of needs in a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently Availability for control is critical, while monitoring individual equipment is less critical Confidentiality is not very important	Customer safety Device standards Cyber Security

Category: Distribution Automation

Scenario: Distribution Automation (DA) Using Local Automation

Category Description

A broad definition of Distribution Automation includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/var control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.
Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Local automation of feeder equipment consists of power equipment that is managed locally by computer-based controllers which are preset with various parameters to issue control actions. These controllers may just monitor power system measurements locally, or may include some short range communications to other controllers and/or local field crews. However, in these scenarios, no communications exist between the feeder equipment and the control center.
Local Automated Switch Management
Local Volt/Var Control
Local Field Crew Communications to Underground Network Equipment

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently Availability for control is critical, while monitoring individual equipment is less critical Confidentiality is not very important	Customer safety Customer device standards Demand response acceptance by customers

Category: Distribution Automation

Scenario: Distribution Automation (DA) Monitoring and Controlling Feeder Equipment

Category Description

A broad definition of Distribution Automation includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/var control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.
Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Operators and distribution applications can monitor the equipment on the feeders and determine whether any actions should be taken to increase reliability, improve efficiency, or respond to emergencies. For instance, they can:
Remotely open or close automated switches
Remotely switch capacitor banks in and out
Remotely raise or lower voltage regulators
Block local automated actions
Send updated parameters to feeder equipment
Interact with equipment in underground distribution vaults
Retrieve power system information from Smart Meters
Automation of Emergency Response
Dynamic Rating of Feeders

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently Availability for control is critical, while monitoring individual equipment is less critical Confidentiality is not very important	Customer safety Customer device standards Demand response acceptance by customers

Category: Distribution Automation

Scenario: Fault Detection, Isolation, and Restoration

Category Description

A broad definition of Distribution Automation includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/var control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.
Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

AMI smart meters and distribution automated devices can detect power outages that affect individual customers and larger groups of customers. As customers rely more fundamentally on power (e.g. PEV) and become used to not having to call in outages, outage detection, and restoration will be come increasingly critical.
The automated fault location, isolation, and service restoration function uses the combination of the power system model with the SCADA data from the field on real-time conditions to determine where a fault is probably located, by undertaking the following steps:
Determines the faults cleared by controllable protective devices:
Determines the faulted sections based on SCADA fault indications and protection lockout signals
Estimates the probable fault locations, based on SCADA fault current measurements and real-time fault analysis
Determines the fault-clearing non-monitored protective device
Uses closed-loop or advisory methods to isolate the faulted segment.
Once the fault is isolated, it determines how best to restore service to unfaulted segments through feeder reconfiguration.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity of outage information is critical Availability to detect large scale outages usually involve multiple sources of information Confidentiality is not very important	Customer safety Customer device standards Demand response acceptance by customers

Category: Distribution Automation

Scenario: Load Management

Category Description

A broad definition of Distribution Automation includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/var control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.
Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Load management provides active and passive control by the utility of customer appliances (e.g. cycling of air conditioner, water heaters, and pool pumps) and certain C&I customer systems (e.g. plenum pre-cooling, heat storage management).
Direct load control and load shedding
Demand side management
Load shift scheduling
Curtailment planning
Selective load management through Home Area Networks

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity of load control commands is critical to avoid unwarranted outages Availability for load control is important – in aggregate (e.g. > 300 MW), it can be critical Confidentiality is not very important	Customer safety Customer device standards Demand response acceptance by customers

Category: Distribution Automation

Scenario: Distribution Analysis using Distribution Power Flow Models

Category Description

A broad definition of Distribution Automation includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/var control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.
Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

The brains behind the monitoring and controlling of field devices are the DA analysis software applications. These applications generally use models of the power system to validate the raw data, assess real-time and future conditions, and issue the appropriate actions. The applications may be distributed and located in the field equipment for local assessments and control, and/or may be centralized in a Distribution Management System for global assessment and control.
Local peer-to-peer interactions between equipment
Normal distribution operations using the Distribution System Power Flow (DSPF) model
Emergency distribution operations using the DSPF model
Study-Mode Distribution System Power Flow (DSPF) model
DSPF /DER Model of distribution operations with significant DER generation/storage

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is critical to operate the distribution power system reliably, efficiently, and safely Availability is critical to operate the distribution power system reliably, efficiently, and safely Confidentiality is not important	Customer safety Customer device standards Demand response acceptance by customers

Category: Distribution Automation

Scenario: Distributed Energy Resource (DER) Management

Category Description

A broad definition of Distribution Automation includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/var control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.
Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

In the future, more and more of generation and storage resources will be connected to the distribution network and will significantly increase the complexity and sensitivity of distribution operations. Therefore, the management of DER generation will become increasingly important in the overall management of the distribution system, including load forecasts, real-time monitoring, feeder reconfiguration, virtual and logical microgrids, and distribution planning.
Direct monitoring and control of DER
Shut-down or islanding verification for DER
Plug-in Hybrid Vehicle (PEV) management, as load, storage, and generation resource
Electric storage fill/draw management
Renewable energy DER with variable generation
Small fossil resource management, such as backup generators to be used for peak shifting

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is critical for any management/ control of generation and storage Availability requirements may vary depending on the size (individual or aggregate) of the DER plant Confidentiality may involve some privacy issues with customer-owned DER	Customer safety Customer device standards Demand response acceptance by customers

Category: Distribution Automation

Scenario: Distributed Energy Resource (DER) Management

Category Description

A broad definition of Distribution Automation includes any automation which is used in the planning,

engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/var control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.
Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Distribution planning typically uses engineering systems with access only to processed power system data that is available from the control center. It is therefore relatively self-contained.
Operational planning
Assessing Planned Outages
Storm Condition Planning
Short-term distribution planning
Short-Term Load Forecast
Short-Term DER Generation and Storage Impact Studies
Long-term distribution planning
Long-Tem Load Forecasts by Area
Optimal Placements of Switches, Capacitors, Regulators, and DER
Distribution System Upgrades and Extensions
Distribution Financial Planners

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity not critical due to multiple sources of data Availability is not important Confidentiality is not important	Cyber security

Category: Plug In Hybrid Electric Vehicles (PHEV)

Scenario: Customer Connects Plug In Hybrid Electric Vehicle to Energy Portal

Category Description

Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging and the use of electric vehicles as a distributed resource.

Scenario Description

This scenario discusses the simple case of a customer plugging in an electric vehicle at their premise to charge its battery. Variations of this scenario will be considered that add complexity: a customer charging their vehicle at another location and providing payment or charging at another location where the premise owner pays.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets Provides power quality for the digital economy Optimizes asset utilization and operate efficiently	The customer's information is kept private Billing information is accurate	Vehicle standards Customer safety Customer device standards Demand response acceptance by customers

Category: Plug In Hybrid Electric Vehicles (PHEV)

Scenario: Customer Connects Plug In Hybrid Electric Vehicle to Energy Portal and Participates in 'Smart' (Optimized) Charging

Category Description

Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging and the use of electric vehicles as a distributed resource.

Scenario Description

In addition to simply plugging in an electric vehicle for charging, in this scenario the electric vehicle charging is optimized to take advantage of lower rates or help prevent excessive load peaks on the electrical system.		
Smart Grid Characteristics	**Objectives/Requirements**	**Potential Stakeholder Issues**
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets Provides power quality for the digital economy Optimizes asset utilization and operate efficiently	Customer information is kept private	Vehicle standards Customer safety Customer device standards Demand response acceptance by customers
Category: Plug In Hybrid Electric Vehicles (PHEV)		
Scenario: Plug In Hybrid Electric Vehicle or Customer Receives and Responds to Discrete Demand Response Events		
Category Description Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging and the use of electric vehicles as a distributed resource.		
Scenario Description An advanced scenario for electric vehicles is the use of the vehicle to provide energy stored in its battery back to the electrical system. Customers could participate in demand response programs where they are provided an incentive to allow the utility to request power from the vehicle at times of high system load.		
Smart Grid Characteristics	**Objectives/Requirements**	**Potential Stakeholder Issues**
Enables active participation by	Improved system stability and	Vehicle standards

consumers Accommodates all generation and storage options Enables new products, services and markets Provides power quality for the digital economy Optimizes asset utilization and operate efficiently	availability To keep customer information private To insure DR messages are accurate and trustworthy	Customer safety Customer device standards Demand response acceptance by customers
Category: Plug In Hybrid Electric Vehicles (PHEV)		
Scenario: Plug In Hybrid Electric Vehicle or Customer Receives and Responds to Utility Price Signals		
Category Description Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging and the use of electric vehicles as a distributed resource.		
Scenario Description In this scenario, the electric vehicle is able to receive and act on electricity pricing data sent from the utility. The use of pricing data for charging is primarily covered in another scenario. The pricing data can also be used in support of a distributed resource program where the customer allows the vehicle to provide power to the electric grid based on market conditions.		
Smart Grid Characteristics Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets Provides power quality for the digital economy Optimizes asset utilization and operate efficiently	**Objectives/Requirements** Improved system stability and availability Pricing signals are accurate and trustworthy Customer information is kept private	**Potential Stakeholder Issues** Vehicle standards Customer safety Customer device standards Demand response acceptance by customers

Category: Distributed Resources

Scenario: Customer Provides Distributed Resource

Category Description

Traditionally, distributed resources have served as a primary or emergency back-up energy source for customers that place a premium on reliability and power quality. Distributed resources include generation and storage devices that can provide power back to the electric power system. Societal, policy and technological changes are increasing the adoption rate of distributed resources and smart grid technologies can enhance the value of these systems.

Scenario Description

This scenario describes the process of connecting a distributed resource to the electric power system and the requirements of net metering.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets Provides power quality for the digital economy Optimizes asset utilization and operate efficiently	Customer information is kept private Net metering is accurate and timely	Safety Customer data privacy and security

Category: Distributed Resources

Scenario: Utility Controls Customer's Distributed Resource

Category Description

Traditionally, distributed resources have served as a primary or emergency back-up energy source for customers that place a premium on reliability and power quality. Distributed resources include generation and storage devices that can provide power back to the electric power system. Societal, policy and technological changes are increasing the adoption rate of distributed resources and smart grid technologies can enhance the value of these systems.

Scenario Description

Distributed generation and storage can be used as a demand response resource where the utility can request or control devices to provide energy back to the electrical system. Customers enroll in utility programs that allow their distributed resource to be used for load support or to assist in maintaining power quality. The utility programs can be based on direct control signals or pricing information.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets Provides power quality for the digital economy Optimizes asset utilization and operate efficiently	Commands are trustworthy and accurate Customer's information is kept private DR messages are received timely	Safety Customer data privacy and security

Category: Transmission Operations

Scenario: Real-time Normal Transmission Operations Using EMS Applications and SCADA Data

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The Energy Management System (EMS) assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers, if power system anomalies are detected.

Scenario Description

Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and Energy Management System. The types of information exchanged include: Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy)

Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies Automation system controls voltage, var and power flow based on algorithms, real-time data, and network linked capacitive and reactive components		
Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is vital to the safety and reliability of the transmission system Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second) Confidentiality is not important	Customer safety Customer device standards Demand response acceptance by customers
Category: Transmission Operations		
Scenario: EMS Network Analysis Based on Transmission Power Flow Models		
Category Description Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The Energy Management System (EMS) assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers, if power system anomalies are detected.		
Scenario Description Energy Management Systems (EMS) assesses the state of the transmission power system using the transmission power system analysis models and the SCADA data from the transmission substations. EMS performs model update, state estimation, bus load forecast EMS performs contingency analysis, recommends preventive and corrective actions EMS performs optimal power flow analysis, recommends optimization actions EMS or planners perform stability study of network Exchange power system model information with RTOs/ISOs and/or other utilities		
Smart Grid	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**

Characteristics Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is vital to the reliability of the transmission system Availability is critical to react to contingency situations via operator commands (e.g. one second) Confidentiality is not important	Cyber Security
Category: Transmission Operations		
Scenario: Real-Time Emergency Transmission Operations		
Category Description Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The Energy Management System (EMS) assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers, if power system anomalies are detected.		
Scenario Description During emergencies, the power system takes some automated actions and the operators can also take actions: Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, LTC control/blocking, shunt control, series compensation control, system separation detection, and wide area real time instability recovery Operators manage emergency alarms SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real time data from equipment monitors, and pre-arming of fast acting emergency automation SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts): Operators performs system restorations based on system restoration plans prepared (authorized) by operation management		
Smart Grid Characteristics	**Cyber Security Objectives/Requirements** Integrity is vital to the safety and reliability of	**Potential Stakeholder Issues** Customer safety

Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	the transmission system Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second) Confidentiality is not important	Customer device standards Demand response acceptance by customers

Category: Transmission Operations

Scenario: Wide Area Synchro-Phasor System

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The Energy Management System (EMS) assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers, if power system anomalies are detected.

Scenario Description

The Wide Area Synchro-Phasor system provides synchronized and time-tagged voltage and current phasor measurements to any protection, control, or monitoring function that requires measurements taken from several locations, whose phase angles are measured against a common, system wide reference. Present day implementation of many protection, control, or monitoring functions are hobbled by not having access to the phase angles between local and remote measurements. With system wide phase angle information, they can be improved and extended. The essential concept behind this system is the system wide synchronization of measurement sampling clocks to a common time reference.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is vital to the safety and reliability of the transmission system Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second) Confidentiality is not important	Cyber Security Customer data privacy and security

Category: RTO/ISO Operations		
Scenario: RTO/ISO Management of Central and DER Generators and Storage		
Category Description		
Scenario Description RTOs and ISOs manage the scheduling and dispatch of central and distributed generation and storage. These functions include: Real time scheduling with the RTO/ISO (for non-market generation/storage) Real time commitment to RTO/ISO Real time dispatching by RTO/ISO for energy and ancillary services Real time plant operations in response to RTO/ISO dispatch commands Real time contingency and emergency operations Black Start (system restoration after blackout) Emissions monitoring and control		
Smart Grid Characteristics Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	**Cyber Security Objectives/Requirements** Integrity is vital to the safety and reliability of the transmission system Availability is critical to operator commands (e.g. one second) Confidentiality is not important	**Potential Stakeholder Issues** Cyber Security Customer data privacy and security

Category: Asset Management
Scenario: Utility gathers circuit and/or transformer load profiles
Category Description At a high level Asset Management seeks a balance between asset performance, cost and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain and protect utility assets.

For our purposes we will establish the scope for the Asset Management category to be the use of specific applications and devices by utility staff such as condition monitoring equipment, protection equipment, event recorders, computer-based maintenance management systems (CMMS), display applications, ratings databases, analysis applications and data marts (historians).

Scenario Description

Load profile data is important for the utility planning staff and is also used by the asset management team that is monitoring the utilization of the assets and by the SCADA/EMS and system operations team. This scenario involves the use of field devices that measure loading, the communications network that delivers the data, the historian database and the load profile application and display capability that is either separate or an integrated part of the SCADA/EMS.

Load profile data may also be used by automatic switching applications that use load data to ensure new system configurations do not cause overloads.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Provides power quality for the range of needs in a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	Data is accurate (integrity) Data is provided timely Customer data is kept private	Customer data privacy and security Cyber Security

Category: Asset Management

Scenario: Utility makes decisions on asset replacement based on a range of inputs including comprehensive off line and on line condition data and analysis applications

Category Description

At a high level Asset Management seeks a balance between asset performance, cost and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain and protect utility assets.

For our purposes we will establish the scope for the Asset Management category to be the use of specific applications and devices by utility staff such as condition monitoring equipment, protection equipment, event recorders, computer-based maintenance management systems (CMMS), display applications, ratings databases, analysis applications and data marts (historians).

Scenario Description

When decisions on asset replacement become necessary the system operator, asset management, apparatus engineering and maintenance engineering staff work closely together with the objective of maximizing the life and utilization of the asset while avoiding an unplanned outage and damage to the equipment.

This scenario involves the use of on-line condition monitoring devices for the range of assets monitored, off line test results, mobile work force technologies, the communications equipment used to collect the on-line data, data marts (historian databases) to store and trend data as well as condition analysis applications, CMMS applications, display applications and SCADA/EMS.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Provides power quality for the range of needs in a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	Data provided is accurate and trustworthy Data is provided timely	Cyber Security Customer data privacy and security

Category: Asset Management

Scenario: Utility performs localized load reduction to relieve circuit and/or transformer overloads

Category Description

At a high level Asset Management seeks a balance between asset performance, cost and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain and protect utility assets.

For our purposes we will establish the scope for the Asset Management category to be the use of specific applications and devices by utility staff such as condition monitoring equipment, protection equipment, event recorders, computer-based maintenance management systems (CMMS), display applications, ratings databases, analysis applications and data marts (historians).

Advanced functions that are associated with Asset Management include dynamic rating and end of life estimation.

Scenario Description

Transmission capacity can become constrained due to a number of system level scenarios and result in an overload situation on lines and substation equipment. Circuit and/or transformer overloads at the distribution level can occur when higher than anticipated customer loads are placed on a circuit or when operator or automatic switching actions are implemented to change the network configuration.

Traditional load reduction systems are used to address generation shortfalls and other system wide issues. Localized load reduction can be a key tool enabling the operator to temporarily curtail the load in a specific area to reduce the impact on specific equipment. This scenario describes the integrated use of the AMI system, the demand response system, other load reduction systems and the SCADA/EMS to achieve this goal.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Provides power quality for the range of needs in a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	Load reduction messages are accurate and trustworthy Customer's information is kept private DR messages are received and processed timely	Demand response acceptance by customers Customer data privacy and security Retail Electric Supplier access Customer data access

Category: Asset Management

Scenario: Utility system operator determines level of severity for an impending asset failure and takes corrective action

Category Description

At a high level Asset Management seeks a balance between asset performance, cost and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain and protect utility assets.

For our purposes we will establish the scope for the Asset Management category to be the use of

specific applications and devices by utility staff such as condition monitoring equipment, protection equipment, event recorders, computer-based maintenance management systems (CMMS), display applications, ratings databases, analysis applications and data marts (historians).		
Scenario Description When pending asset failure can be anticipated the system operator, asset management, apparatus engineering and maintenance engineering staff work closely together with the objective of avoiding an unplanned outage while avoiding further damage to the equipment. This scenario involves the use of on-line condition monitoring devices for the range of assets monitored, off line test results, mobile work force technologies, the communications equipment used to collect the on-line data, data marts (historian databases) to store and trend data as well as condition analysis applications, CMMS applications, display applications and SCADA/EMS.		
Smart Grid Characteristics	**Objectives/Requirements**	**Potential Stakeholder Issues**
Provides power quality for the range of needs in a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	Asset information provided is accurate and trustworthy Asset information is provided timely	Cyber Security Customer data privacy and security

APPENDIX B
CROSSWALK OF CYBER SECURITY DOCUMENTS

The following is a mapping between the security requirements contained in several relevant documents that include security requirements that may be applicable to the Smart Grid. All of the documents listed in this table will be used as source documents in the selection and tailoring of the security requirements for the Smart Grid.

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
Access Control					
AC-1	Access Control Policy and Procedures	2.9.6 2.9.7 2.15.1	Information and Document Classification Information and Document Retrieval Access Control Policies and Procedures	CIP 003 (R4, R4.1, R4.2) CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)	3.2.2
AC-2	Account Management	2.2.6 2.15.6	Termination of Third Party Access Supervision and Review	CIP 004-2 (R4) CIP 007-2 (R5.1.2)	
AC-3	Access Enforcement	2.9.6 2.15.7	Information and Document Classification Access Enforcement	CIP 003 (R4, R4.1, R4.2) CIP 004-2 (R4) CIP 005-2 (R2, R2.1-R2.4)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
AC-4	Information Flow Enforcement	2.15.3 2.15.15	Account Management Information Flow Enforcement	CIP 003-2 (R5, R5.1, R5.2, 5.3) CIP 004-2 (R4, R4.1, R4.2) CIP 005-2 (R2.5) CIP 007-2 (R5, R5.1, R5.2)	
AC-5	Separation of Duties	2.15.8	Separation of Duties		
AC-6	Least Privilege	2.15.9	Least Privilege	CIP-007-2 (R5.1)	
AC-7	Unsuccessful Login Attempts	2.15.20	Unsuccessful Logon Notification		
AC-8	System Use Notification	2.15.17	System Use Notification	CIP-005-2 (R2.6)	
AC-9	Previous Logon (Access) Notification	2.15.19	Previous Logon Notification		
AC-10	Concurrent Session Control	2.15.18	Concurrent Session Control		
AC-11	Session Lock	2.15.21	Session Lock		
AC-12	Session Termination (Withdrawn)				
AC-13	Supervision and Review—Access Control (Withdrawn)				

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
AC-14	Permitted Actions without Identification or Authentication	2.15.11	Permitted Actions without Identification and Authentication		
AC-15	Automated Marking (Withdrawn)				
AC-16	Security Attributes	2.9.11	Automated labeling		
AC-17	Remote Access	2.15.23 2.15.24	Remote Access Policy and Procedures Remote Access	CIP 005-2 (R1, R1.1, R1.2, R2, R2.3, R2.4 CIP 005-2 (R2, R3, R3.1, R3.2	
AC-18	Wireless Access	2.15.26	Wireless Access Restrictions		6.3.2.5
AC-19	Access Control for Mobile Devices	2.15.25	Access Control for Portable and Mobile Devices	CIP 005-2 (R2.4, R5, R5.1)	6.2.2.2
AC-20	Use of External Information Systems	2.15.29 2.15.27	Use of External Information Control Systems Personally Owned Information		
AC-21	User-Based Collaboration and Information Sharing				
AC-22	Publicly Accessible Content	2.15.30	Publicly Accessible Content		

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	2.11.1	Security Awareness Training Policy and Procedures	CIP 004-2 (R1, R2)	
AT-2	Security Awareness	2.11.2	Security Awareness	CIP 004-2 (R1)	
AT-3	Security Training	2.7.5 2.11.3	Planning Process Training Security Training	CIP 004-2 (R2) CIP 004-2 (R2)	
AT-4	Security Training Records	2.11.4	Security Training Records	CIP 004-2 (R2.3)	
AT-5	Contacts with Security Groups and Associations	2.11.5	Contact with Security Groups and Associations		
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	2.16.1	Audit and Accountability Process and Procedures	CIP 003-2 (R1, R1.1, R1.3)	4.2 6.3.3
AU-2	Auditable Events	2.16.2	Auditable Events	CIP 005-2 (R3) CIP 007-2 (R5.1.2, R5.2.3, R6.1, R6.3)	6.3.3
AU-3	Content of Audit Records	2.16.3	Content of Audit Records	CIP 007-2 (R5.1.2)	6.3.3
AU-4	Audit Storage Capacity	2.16.4	Audit Storage Capacity		
AU-5	Response to Audit Processing Failures	2.16.5	Response to Audit Processing Failures		
AU-6	Audit Review, Analysis, and	2.15.6	Supervision and Review	CIP 007-2 (R5.1.2)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
	Reporting	2.16.6	Audit Monitoring, Analysis, and Reporting	CIP 007-2 (R6.5)	6.3.3
AU-7	Audit Reduction and Report Generation	2.16.7	Audit Reduction and Report Generation		6.3.3
AU-8	Time Stamps	2.16.8	Time Stamps		6.3.3
AU-9	Protection of Audit Information	2.16.9	Protection of Audit Information	CIP 003-2 (R4)	6.3.3
AU-10	Non-repudiation	2.16.16	Non-Repudiation		
AU-11	Audit Record Retention	2.16.10	Audit Record Retention	CIP 005-2 (R5.3) CIP 007-2 (R5.1.2, R6.4) CIP 008-2 (R.2)	6.3.3
AU-12	Audit Generation	2.16.15	Audit Generation		
AU-13	Monitoring for Information Disclosure				
AU-14	Session Audit				
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures		
CA-2	Security Assessments	2.7.6 2.10.3	Testing System Monitoring and Evaluation	CIP 007-2 (R1) CIP 007-2 (R8)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
		2.16.11	Conduct and Frequency of Audits		6.3.1
		2.16.14	Security Policy Compliance		
		2.17.3	Monitoring of Security Policy		
		2.17.6	Security Certification		
		2.18.4	Security Assessments	CIP 007-2 (R1)	
CA-3	Information System Connections	2.8.18	System Connections	CIP 005-2 (R2, R2.2-R2.4)	
		2.18.5	Control System Connections	CIP 005-2 (R2)	
CA-4	Security Certification (Withdrawn)				
CA-5	Plan of Action and Milestones	2.18.6	Plan of Action and Milestones	CIP 005-2 (R4.5) CIP 007-2 (R8.4)	
CA-6	Security Authorization	2.17.5	Security Accreditation		
CA-7	Continuous Monitoring	2.7.9	Risk Mitigation	CIP 002-2 (R1)	
		2.10.3	System Monitoring and Evaluation.	CIP 007-2 (R8)	
		2.16.11	Conduct and Frequency of Audits		6.3.1
		2.16.14	Security Policy Compliance		
		2.18.7	Continuous Monitoring		

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
Configuration Management					
CM-1	Configuration Management Policy and Procedures	2.6.1	Configuration Management Policy and Procedures	CIP 003-2 (R6)	
CM-2	Baseline Configuration	2.6.2	Baseline Configuration	CIP-2 007 (R9)	
CM-3	Configuration Change Control	2.6.3	Configuration Change Control	CIP 003-2 (R6)	
CM-4	Security Impact Analysis	2.6.4	Monitoring Configuration Changes	CIP 003-2 (R6)	
CM-5	Access Restrictions for Change	2.6.5	Access Restrictions for Configuration Change	CIP 003-2 (R6)	
CM-6	Configuration Settings	2.6.6	Configuration Settings	CIP 003-2 (R6) CIP 005 (R2.2)	
CM-7	Least Functionality	2.6.7	Configuration for Least Functionality		
CM-8	Information System Component Inventory	2.6.8	Configuration Assets		
CM-9	Configuration Management Plan	2.6.11	Configuration Management Plan		
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures				
CP-2	Contingency Plan	2.12.2	Continuity of Operations Plan	CIP 008-2 (R1) CIP 009-2 (R1)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
		2.12.3 2.12.6	Continuity of Operations Roles and Responsibilities Continuity of Operations Plan Update	CIP 009-2 (R1.1, R1.2) CIP 009-2 (R3)	6.2.3
CP-3	Contingency Training				
CP-4	Contingency Plan Testing and Exercises	2.12.5	Continuity of Operations Plan Testing	CIP 008-2 (R1.6) CIP 009-2 (R2, R5)	6.2.3 6.2.3.2
CP-5	Contingency Plan Update (Withdrawn)				
CP-6	Alternate Storage Site	2.12.13	Alternative Storage Sites		
CP-7	Alternate Processing Site	2.12.14	Alternate Command/Control Methods		
		2.12.15	Alternate Control Center		
CP-8	Telecommunications Services	2.12.15	Alternate Control Center		
		2.12.14	Alternate Command/Control Methods		
CP-9	Information System Backup	2.10.4 2.12.16	Backup and Recovery Control System Backup	CIP 009-2 (R4) CIP 009-2 (R4, R5)	6.2.3
CP-10	Information System Recovery and	2.10.4	Backup and Recovery	CIP 009-2 (R4)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
	Reconstitution	2.12.17	Control System Recovery and Reconstitution	CIP 009-2 (R4)	6.2.3.2
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	2.15.2	Identification and Authentication Procedures and Policy	CIP 003-2 (R1, R1.1, R1.3)	
IA-2	Identification and Authentication (Organizational Users)	2.15.10	User Identification and Authentication	CIP 005-2 (R2,)	
IA-3	Device Identification and Authentication	2.15.12	Device Authentication and Identification		
IA-4	Identifier Management	2.15.4	Identifier Management		
IA-5	Authenticator Management	2.6.10 2.15.5 2.15.16	Factory Default Authentication Management Authenticator Management Passwords	CIP 005-2 (R4.4) CIP 007-2 (R5, R5.1, R5.2, R5.3) CIP 007-2 (R5.3)	
IA-6	Authenticator Feedback				
IA-7	Cryptographic Module Authentication				
IA-8	Identification and Authentication (Non-Organizational Users)				
Incident Response					

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
IR-1	Incident Response Policy and Procedures	2.7.4 2.12.1	Incident Roles and Responsibilities Incident Response Policy and Procedures	CIP 008-2 (R1.2) CIP 009-2 (R1.2) CIP 008-2 (R1, R1.2-R1.5)	6.1.1
IR-2	Incident Response Training	2.7.4 2.12.4	Incident Roles and Responsibilities Incident Response Training	CIP 008-2 (R1.2) CIP 009-2 (R1.2) CIP 009-2 (R2)	
IR-3	Incident Response Testing and Exercises	2.12.5	Continuity of Operations Plan Testing	CIP 008-2 (R1.6) CIP 009-2 (R2, R5)	6.2.3 6.2.3.2
IR-4	Incident Handling	2.7.7 2.7.8 2.12.7 2.12.12	Investigate and Analyze Corrective Action Incident Handling Corrective Action	CIP 008-2 (R1) CIP 009 (R3) CIP 008-2 (R1.1, R1.2, R1.3) CIP 008-2 (R1.4) CIP 009-2 (R3)	
IR-5	Incident Monitoring	2.12.8	Incident Monitoring	CIP 007-2 (R6, R6.2)	
IR-6	Incident Reporting	2.12.9	Incident Reporting	CIP 008-2 (R1.3)	
IR-7	Incident Response Assistance	2.12.10	Incident Response Assistance	CIP 008-2 (R1, R1.2, R1.3)	
IR-8	Incident Response Plan	2.7.3	Interruption Identification and Classification		

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
		2.12.11	Incident Response Investigation and Analysis	CIP 008-2 (R1)	
		2.12.12	Corrective Action	CIP 008-2 (R1.4) CIP 009-2 (R3)	
Maintenance					
MA-1	System Maintenance Policy and Procedures	2.10.1	System Maintenance Policy and Procedures		
MA-2	Controlled Maintenance	2.10.6	Periodic System Maintenance		
MA-3	Maintenance Tools	2.10.7	Maintenance Tools		
MA-4	Non-Local Maintenance	2.10.9	Remote Maintenance		
MA-5	Maintenance Personnel	2.10.8	Maintenance Personnel		
MA-6	Timely Maintenance	2.10.10	Timely Maintenance	CIP 009-2 (R4)	
Media Protection					
MP-1	Media Protection Policy and Procedures	2.9.3	Information Handling	CIP 003-2 (R4.1)	
		2.9.6	Information and Document Classification	CIP 003 (R4, R4.1, R4.2)	
		2.13.1	Media Protection and Procedures		3.3.2
MP-2	Media Access	2.13.2	Media Access		3.3.2
MP-3	Media Marking	2.9.10	Automated Marking		
		2.13.3	Media Classification	CIP 003-2 (R4)	6.2.1 6.2.2

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
		2.13.4	Media Labeling		
MP-4	Media Storage	2.13.5	Media Storage		
MP-5	Media Transport	2.13.6	Media Transport		
MP-6	Media Sanitization	2.6.9 2.9.8 2.13.7	Addition, Removal, and Disposition of Equipment Information and Document Destruction Media Sanitization and Storage	CIP 003-2 (R6) CIP 007-2 (R7, R7.1, R7.2, R7.3)	6.2.7
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	2.4.1	Physical and Environmental Security Policies and Procedures	CIP 006-2 (R1, R2)	6.2.2
PE-2	Physical Access Authorizations	2.4.2	Physical Access Authorizations	CIP 004-2 (R4)	
PE-3	Physical Access Control	2.4.3	Physical Access Control	CIP 006-2 (R2)	6.2.2
		2.4.21	Physical Device Access Control	CIP 006-2 (R2, R3)	
PE-4	Access Control for Transmission Medium				
PE-5	Access Control for Output Devices				
PE-6	Monitoring Physical Access	2.4.4	Monitoring Physical Access	CIP 006-2 (R5)	6.2.2

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
PE-7	Visitor Control	2.4.5	Visitor Control	CIP 006-2 (R1.4)	
PE-8	Access Records	2.4.6 2.4.7	Visitor Records Physical Access Log Retention	CIP 006-2 (R1.4, R6) CIP 006-2 (R7)	
PE-9	Power Equipment and Power Cabling	2.4.20	Power Equipment and Power Cabling		6.2.2.3
PE-10	Emergency Shutoff	2.4.8	Emergency Shutoff		6.2.2
PE-11	Emergency Power	2.4.9	Emergency Power		
PE-12	Emergency Lighting	2.4.10	Emergency Lighting		
PE-13	Fire Protection	2.4.11	Fire Protection		
PE-14	Temperature and Humidity Controls	2.4.12	Temperature and Humidity Controls		
PE-15	Water Damage Protection	2.4.13	Water Damage Protection		
PE-16	Delivery and Removal	2.4.14	Delivery and Removal		
PE-17	Alternate Work Site	2.4.15	Alternate Work Site		6.2.2.1
PE-18	Location of Information System Components	2.4.18	Location of Control System Assets		
PE-19	Information Leakage				
Planning					

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
PL-1	Security Planning Policy and Procedures	2.7.1	Strategic Planning Policy and Procedures		
PL-2	System Security Plan	2.7.2 2.7.9 2.7.10	Control System Security Plan Risk Mitigation System Security Plan Update	CIP 002-2 (R1)	6.1.2
PL-3	System Security Plan Update (Withdrawn)				
PL-4	Rules of Behavior	2.7.11	Rules of Behavior		
PL-5	Privacy Impact Assessment				
PL-6	Security-Related Activity Planning	2.7.12	Security-Related Activity Planning	CIP 007-2 (R1.1)	
Personnel Security					
PS-1	Personnel Security Policy and Procedures	2.3.1	Personnel Security Policies and Procedures	CIP 004-2 (R3)	6.2.1
PS-2	Position Categorization	2.3.2	Position Categorization	CIP 004-2 (R3)	
PS-3	Personnel Screening	2.3.3	Personnel Screening	CIP 004-2 (R3)	6.2.1
PS-4	Personnel Termination	2.2.6 2.3.4	Termination of Third Party Access Personnel Termination	CIP 004-2 (R4) CIP 004-2 (R4.2) CIP 007-2 (R5.2.3)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
PS-5	Personnel Transfer	2.3.5	Personnel Transfer	CIP 004-2 (R4.1, R4.2)	
PS-6	Access Agreements	2.3.6	Access Agreements		
PS-7	Third-Party Personnel Security	2.3.7	Third Party Personnel Security	CIP 004-2 (R3.3)	
PS-8	Personnel Sanctions	2.3.8	Personnel Accountability		
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	2.18.1	Risk Assessment Policy and Procedures	CIP 002-2 (R1, R1.1, R1.2, R4) CIP 003-2 (R1, R1.3)	6.1.1
RA-2	Security Categorization	2.9.4	Information Classification	CIP 003-2 (R4, R4.2)	
RA-3	Risk Assessment	2.18.9 2.18.10 2.18.12	Risk Assessment Risk Assessment Update Identify, Classify, Analyze, and Prioritize Potential Security Risks	CIP 002-2 (R1.2) CIP 002-2 (R4)	
RA-4	Risk Assessment Update (Withdrawn)				
RA-5	Vulnerability Scanning	2.10.3	System Monitoring and Evaluation	CIP 007-2 (R8)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
		2.18.11	Vulnerability Assessment and Awareness	CIP 005-2 (R4, R4.2, R4.3, R4.4) CIP 007-2 (R8)	
System and Service Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	2.5.1	System and Services Acquisition Policy and Procedures		
SA-2	Allocation of Resources	2.5.2	Allocation of Resources		
SA-3	Life Cycle Support	2.5.3 2.8.19	Life-Cycle Support Security Roles	CIP 003-2 (R5)	
SA-4	Acquisitions	2.5.4	Acquisitions		
SA-5	Information System Documentation	2.5.5	Control System Documentation		
SA-6	Software Usage Restrictions	2.5.6	Software License Usage Restrictions		
SA-7	User-Installed Software	2.5.7	User-installed Software		
SA-8	Security Engineering Principles	2.5.8	Security Engineering Principals		
SA-9	External Information System Services	2.5.9 2.8.19	Outsourced Control System Services Security Roles	CIP 003-2 (R5)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
SA-10	Developer Configuration Management	2.5.10	Vendor Configuration Management		
SA-11	Developer Security Testing	2.5.11	Vendor Security Testing		
SA-12	Supply Chain Protection	2.5.12	Supply Chain Protection		
SA-13	Trustworthiness	2.5.13	Trustworthiness		
SA-14	Critical Information System Components				
System and Communication Protection					
SC-1	System and Communications Protection Policy and Procedures	2.8.1	System and Communication Protection Policy and Procedures	CIP 003-2 (R1, R1.1, R1.3)	
SC-2	Application Partitioning	2.8.2 2.8.32	Management Port Partitioning Application Partitioning		
SC-3	Security Function Isolation	2.8.3	Security Function Isolation		
SC-4	Information in Shared Resources	2.8.4	Information Remnants		
SC-5	Denial of Service Protection	2.8.5	Denial-of-Service Protection		
SC-6	Resource Priority	2.8.6	Resource Priority		

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
SC-7	Boundary Protection	2.8.7	Boundary Protection	CIP 005-2 (R1, R1.1, R1.2, R1.3, R1.4, R1.6, R2, R2.1-R2.4, R5, R5.1)	
SC-8	Transmission Integrity	2.8.8	Communication Integrity		
SC-9	Transmission Confidentiality	2.8.9	Communication Confidentially		
SC-10	Network Disconnect	2.15.22	Remote Session Termination		
SC-11	Trusted Path	2.8.10	Trusted Path		
SC-12	Cryptographic Key Establishment and Management	2.8.11	Cryptographic Key Establishment and Management		
SC-13	Use of Cryptography	2.8.12	Use of Validated Cryptography		
SC-14	Public Access Protections	2.8.4	Information Remnants		
SC-15	Collaborative Computing Devices	2.8.13	Collaborative Computing		
SC-16	Transmission of Security Attributes	2.8.14	Transmission of Security Parameters		
SC-17	Public Key Infrastructure Certificates	2.8.15	Public Key Infrastructure Certificates		
SC-18	Mobile Code	2.8.16	Mobile Code		

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
SC-19	Voice Over Internet Protocol	2.8.17	Voice-over-Internet Protocol		
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	2.8.22	Secure Name/Address Resolution Service (Authoritative Source)		
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver)		
SC-22	Architecture and Provisioning for Name/Address Resolution Service	2.8.21	Architecture and Provisioning for Name/Address Resolution Service		
SC-23	Session Authenticity	2.8.20	Message Authenticity		
SC-24	Fail in Known State	2.12.18 2.8.24	Fail-Safe Response Fail in Known State		5.10
SC-25	Thin Nodes	2.8.25	Thin Nodes		
SC-26	Honeypots	2.8.26	Honeypots		
SC-27	Operating System-Independent Applications	2.8.27	Operating System-Independent Applications		
SC-28	Protection of Information at Rest	2.8.28	Confidentiality of Information at Rest		
SC-29	Heterogeneity	2.8.29	Heterogeneity		
SC-30	Virtualization Techniques	2.8.30	Virtualization Techniques		

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
SC-31	Covert Channel Analysis	2.8.31	Covert Channel Analysis		
SC-32	Information System Partitioning	2.8.33	Information System Partitioning		
SC-33	Transmission Preparation Integrity				
SC-34	Non-Modifiable Executable Programs				
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	2.14.1	System and Information Integrity Policy and Procedures		2.14.1
SI-2	Flaw Remediation	2.14.2	Flaw Remediation	CIP 007-2 (R3, R3.1, R3.2)	
SI-3	Malicious Code Protection	2.14.3	Malicious Code Protection	CIP 007-2 (R4, R4.1, R4.2)	2.14.3
SI-4	Information System Monitoring	2.14.4	System Monitoring Tools and Techniques	CIP 007-2 (R6)	2.14.4
SI-5	Security Alerts, Advisories, and Directives	2.14.5	Security Alerts and Advisories		2.14.5
SI-6	Security Functionality Verification	2.14.6	Security Functionality Verification	CIP 007-2 (R1)	2.14.6
SI-7	Software and Information Integrity	2.14.7	Software and Information Integrity		
SI-8	Spam Protection	2.14.8	Spam Protection	CIP 007-2 (R4)	3.2, 6.2.6

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
SI-9	Information Input Restrictions	2.14.9	Information Input Restrictions	CIP 003-2 (R5) CIP 007-2 (R5, R5.1, 5.2)	
SI-10	Information Input Validation	2.14.10	Information Input Accuracy, Completeness, Validity and Authenticity		
SI-11	Error Handling	2.14.11	Error Handling		
SI-12	Information Output Handling and Retention	2.9.2 2.14.12	Information and Document Retention Information Output Handling and Retention	CIP 006-2 (R7)	
SI-13	Predictable Failure Prevention	2.14.13	Predictable Failure Prevention		
Program Management					
PM-1	Information Security Program Plan	2.1.1	Security Policies and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)	4.2
		2.2.1	Management Policies and Procedures	CIP 003-2 (R1, R2, R3, R4, R5, R6)	ES-3
		2.2.2	Management Accountability	CIP 003-2 (R2, R3)	4.2.1
		2.2.3	Baseline Practices		

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
		2.17.1	Monitoring and Reviewing Control System Security management Policy and Procedures		
		2.19.1	Security Program Plan		
PM-2	Senior Information Security Officer	2.19.2	Senior Security Officer		
PM-3	Information Security Resources	2.19.3	Security Resources		
PM-4	Plan of Action and Milestones Process	2.19.4	Plan of Action and Milestones Process		
PM-5	Information System Inventory	2.19.5	System Inventory		
PM-6	Information Security Measures of Performance	2.19.6	Security Measures of Performance		
PM-7	Enterprise Architecture	2.19.7	Enterprise Architecture		
PM-8	Critical Infrastructure Plan	2.19.8	Critical Infrastructure Plan		
PM-9	Risk Management Strategy	2.2.4	Coordination of Threat Mitigation	CIP 008-2 (R1.3)	
		2.7.3	Interruption Identification and Classification		
		2.7.9	Risk Mitigation	CIP 002-2 (R1)	
		2.18.2	Risk Management Plan	CIP 003-2 (R4, R4.1, R4.2)	

800-53	NIST SP 800-53	DHS Catalog of Control System Security Req	DHS Catalog of Control System Security	NERC CIPs (1-9) May 2009	NIST SP 800-82
		2.19.9	Risk Management Strategy		
PM-10	Security Authorization Process	2.19.10	Security Authorization Process		
PM-11	Mission/Business Process Definition	2.19.11	Mission/Business Process Definition		

APPENDIX C
VULNERABILITY CLASSES

C.1 INTRODUCTION

This chapter is in draft format. For the purpose of this chapter, a Vulnerability Class is a category of weakness which could adversely impact the operation of the electric grid. A "vulnerability" is the thing which can be leveraged to cause disruption or have otherwise undo influence over the Smart Grid. Actual attacks and impacts will be noted in additional documentation still being produced.

We envision this information to be used in discussions specifically by the SGIP-CSWG at large and its various subgroups.

As input to the classification process, we used many sources of vulnerability information, including NIST 800-82 and 800-53, OWASP vulnerabilities, CWE vulnerabilities, attack documentation from INL, input provided by the NIST SGIP-CSWG Bottoms-Up group, and the NERC CIP standards. Compiling one document from these many sources with different view-points has sometimes been challenging, and further refinement is planned based on feedback from the SGIP-CSWG. This document is still under revision and is open for comment.

C.2 PEOPLE, POLICY & PROCEDURE

Policy and Procedure are the documented mechanisms by which an organization operates, and People are trained to follow them. These policies and procedures lay the groundwork for how the organization will operate. This section outlines places where a failure in, or lack of, policy and procedure can lead to a security risk for the organization. Policies and procedures are often the final protective or mitigating control, and they should be examined closely to ensure that they are consistent with both the business objectives and with secure operations.

C.2.1 Training

This category of vulnerabilities is related to personnel training in all forms that relates to implementing, maintaining, and operating systems.

Insufficient Trained Personnel

Description

Throughout the entire organization everyone needs to acquire a level of Security Awareness training, the degree of this training also is varied based on the technical responsibilities and/or the critical asset/s one is responsible for.

Through this training effort everyone gets a clear understanding of the importance of Cyber Security but more important everyone begins to understand the role they play and importance of each role.

Examples

- Freely releasing information of someone's status, i.e. away on vacation, not in today, etc.

- Opening emails and attachments form unknown sources.
- Posting passwords for all to see.

Potential Impact:

As the social engineering element is 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.

Inadequate Security Training and Awareness Program

Description

As part and continuation of Insufficient trained personnel with the one element being that within the Policy framework to highlight the requirement of a continuous/re-train effort over some identified period of time. The Security profile will always be changes so will the need for new procedures, new technologies and re-enforcement of the importance of the cyber security program.

C.2.2 Policy & Procedure

Insufficient Identity Validation, Background Checks

Description

Identity Validation/background levels goes directly to the individual's area of responsibility and the level of information they are given access to. The more sensitive information available to an individual the deeper and more detailed the validation and checking process is needed.

Use of know references and background checking by established groups should be implemented.

Potential Impact

The human factor is always going to be considered the weakest element within any Security posture. But validation and background checking are measures that are imperative to be able manage this element. As the amount of and sensitivity of the information one is given the responsibility of a consideration of multiple signoffs before that information is released, another step in not giving any one individual/s the "keys to the kingdom".

Inadequate Security Policy

Description

Vulnerabilities are often introduced due to inadequate policies or the lack of policies.

Policies need to drive operating requirements and procedures…

Potential Impact

Security policy must be structured with several key elements, must be well understood, must be of a practical approach, must be well in practice and monitored, and must be enforceable.

They must be flexible enough that they can be continuously improved.

Inadequate Privacy Policy

Description

A privacy policy that documents the necessity of protection of private personal information is necessary to ensure that data is not exposed or shared unnecessarily.

Potential Impact

Insufficient privacy policies can lead to unwanted exposure of employee personal or customer/client personal information, leading to both business risk and security risk.

Inadequate Patch Management Process

Description

A patch management process is necessary to ensure that software and firmware are kept current, or that a proper risk analysis and mitigation process is in place when patches cannot be promptly installed.

Potential Impact

Missing patches on firmware and software have the potential to present serious risk to the affected system.

Inadequate Change and Configuration Management

Description

Change and configuration management processes are essential to ensuring that system configurations are governed appropriately in order to maximize overall system reliability.

Examples

- Changing software configuration that enables an insecure profiles
- Adding vulnerable hardware
- Changing network configuration that reduces the security profile of the system
- Introduction of tampered devices into the system
- Security organization not having a sign-off approval in the configuration management process.

Potential Impact

Improperly configured software/systems/devices added to existing software/systems/devices can lead to insecure configurations and increased risk of vulnerability.

Unnecessary System Access

Description

Under policy is needs to be very clear that only access and information is granted on an as need basis, access needs to be well controlled and monitored and again very dependent of the access requirement and level of impact that access could have on an organization.

C.2.3 Risk Management

The vulnerabilities in this section are related to the implementation of a risk management program. Deficiencies in a risk management program can lead to vulnerabilities not only at the technical layer, but at the business decision-making layer as well.

Inadequate Periodic Security Audits

Description

Independent security audits should review and examine a system's records and activities to determine the adequacy of system controls and ensure compliance with established security policy and procedures. Audits should also be used to detect breaches in security services and recommend changes, which may include making existing security controls more robust and/or adding new security controls. Audits should not completely rely on interviews with the systems administrators.

Potential Impact

The Audit process is the only true measure to continuously evaluate the status of the implemented Security Program, from conformance to policy, the need to enhance both policy and/or procedures and evaluate security robustness of your implemented security technologies.

Inadequate Security Oversight by Management

Description

With no clear Senior Management ownership of a Security program, in the event of a policy being compromised or abused it then becomes almost impossible to enforce.

Potential Impact

Within a security program it will require the crossing of many organization operating groups, have impact on many business areas, requires an element of Human Recourses and legal involvement, without a senior management oversight/ownership it makes is very difficult to be successful. The biggest challenge is establishing this senior management oversight at the executive level within an organization.

Inadequate Continuity of Operations or Disaster Recovery Plan

Description

To ensure within the various plant/system disaster recovery plans that are in place that each highlight within their elements that if the disaster was created by a cyber related incident than part of the recovery process has to ensure elements that are focus on a cyber incident recovery.

Here it is the added steps like, validating backups, ensuring devices being recovered are clean before installing the backups, incident reporting, etc…

Potential Impact

Longer than required of a possible plant or operational outage.

Inadequate Risk Assessment Process

Description

A documented assessment process, that includes consideration of business objectives, is necessary to ensure proper evaluation of risk.

Examples

- The NERC Critical Asset identification process

Potential Impact

Lack of risk assessment processes can lead to decisions made without basis in actual risk.

Inadequate Risk Management Process

Description

Unmanaged risk leads to unmanaged vulnerabilities in affected systems.

Potential Impact

Unmanaged risk and/or vulnerabilities can to lead to exploitation of impacted systems.

Inadequate Incident Response Process

Description

An incident response process is required to ensure proper notification and action in the event of an incident.

Potential Impact

Without a sufficient incident response process, response-time critical actions may not be completed in a timely manner, leading to increased duration of exposure.

C.3 PLATFORM SOFTWARE/FIRMWARE VULNERABILITIES

Software and firmware are the programmable components of a computing environment. Errors or oversights in software and firmware design, development, and deployment may result in unintended functionality that allows attackers or other conditions to affect, via programmatic means, the confidentiality, integrity and/or availability of information. This section describes classes and subclasses of vulnerabilities in platform software and firmware. It is important to note that new instances of software and firmware vulnerabilities are continually being discovered. New classes and subclasses of software and firmware vulnerabilities are also discovered from time to time.

C.3.1 Software Development

Applications being developed for use in the Smart Grid should make use of a Secure Software Development Lifecycle. Vulnerabilities in this category can arise from a lack oversight in this area, leading to poor code implementation, leading to vulnerability.

Code Quality Vulnerability

Description

"Poor code quality leads to unpredictable behavior. From a user's perspective that often manifests itself as poor usability. For an attacker it provides an opportunity to stress the system in unexpected ways" (OWASP page).

Examples

- Double Free
- Failure to follow guideline/specification
- Leftover Debug Code
- Memory leak
- Null Dereference
- Poor Logging Practice
- Portability Flaw
- Undefined Behavior
- Uninitialized Variable
- Unreleased Resource
- Unsafe Mobile Code
- Use of Obsolete Methods
- Using freed memory

Arbitrary code execution Authentication Vulnerability

Description

Authentication is the process of proving an identity to a given system. Users, applications, and devices may all require authentication. This class of vulnerability leads to authentication bypass or other circumvention/manipulation of the authentication process.

Examples

- Confidence tricks
- Remote technical tricks
- Local technical tricks

- Victim mistakes
- Implementation oversights
- Denial of service attacks
- Enrollment attacks (OWASP page "Comprehensive list of Threats to Authentication Procedures and Data")
- Allowing password aging
- Authentication Bypass via Assumed-Immutable Data
- Empty String Password
- Failure to drop privileges when reasonable
- Hard-Coded Password
- Not allowing password aging
- Often Misused: Authentication
- Reflection attack in an auth protocol
- Unsafe Mobile Code
- Using password systems
- Using referer field for authentication or authorization
- Using single-factor authentication

Potential Impact

Access granted without official permission

Authorization Vulnerability

Description

Authorization is the process of assigning correct system permissions to an authenticated entity. This class of vulnerability allows authenticated entities the ability to perform actions which policy does not allow.

Examples

- Code Permission Vulnerability
- Access control enforced by presentation layer
- File Access Race Condition: TOCTOU
- Least Privilege Violation
- Often Misused: Privilege Management
- Using referer field for authentication or authorization
- Insecure direct object references

- Failure to restrict URL access

Cryptographic Vulnerability

Description

Cryptography is the use of mathematical principles to ensure that information is hidden from unauthorized parties, the information is unchanged, and the intended party can verify the sender. This vulnerability class includes issues which allow an attacker to view, modify or forge encrypted data, or impersonate another party through digital signature abuse.

Examples

- Algorithm problems
- Key management problems
- Random number generator problems
- Addition of data-structure sentinel
- Assigning instead of comparing
- Comparing instead of assigning
- Deletion of data-structure sentinel
- Duplicate key in associative list
- Failure to check whether privileges were dropped successfully
- Failure to deallocate data
- Failure to provide confidentiality for stored data
- Guessed or visible temporary file
- Improper cleanup on thrown exception
- Improper error handling
- Improper temp file opening
- Incorrect block delimitation
- Misinterpreted function return value
- Missing parameter
- Omitted break statement
- Passing mutable objects to an un-trusted method
- Symbolic name not mapping to correct object
- Truncation error
- Undefined Behavior
- Uninitialized Variable

- Unintentional pointer scaling
- Use of sizeof() on a pointer type
- Using the wrong operator

Environmental Vulnerability

Description

"This category includes everything that is outside of the source code but is still critical to the security of the product that is being created. Because the issues covered by this kingdom are not directly related to source code, we separated it from the rest of the kingdoms." (OWASP page)

Examples

- ASP.NET Misconfigurations
- Empty String Password
- Failure of true random number generator
- Information leak through class cloning
- Information leak through serialization
- Insecure Compiler Optimization
- Insecure Transport
- Insufficient Session-ID Length
- Insufficient entropy in pseudo-random number generator
- J2EE Misconfiguration: Unsafe Bean Declaration
- Missing Error Handling
- Publicizing of private data when using inner classes
- Relative path library search
- Reliance on data layout
- Relying on package-level scope
- Resource exhaustion
- Trust of system event data

Error Handling Vulnerability

Description

Error handling refers to the way an application deals with unexpected conditions - generally syntactical or logical. Vulnerabilities in this class provide means for attackers to use error handling to access unintended information or functionality.

Examples

- ASP.NET Misconfigurations
- Catch NullPointerException
- Empty Catch Block
- Improper cleanup on thrown exception
- Improper error handling
- Information Leakage
- Missing Error Handling
- Often Misused: Exception Handling
- Overly-Broad Catch Block
- Overly-Broad Throws Declaration
- Return Inside Finally Block
- Uncaught exception
- Unchecked Error Condition

General Logic Error

Description

Logic errors are programming missteps that allow an application to operate incorrectly but usually without crashing. This vulnerability class covers those error types that have security implications.

Examples

- Addition of data-structure sentinel
- Assigning instead of comparing
- Comparing instead of assigning
- Deletion of data-structure sentinel
- Duplicate key in associative list
- Failure to check whether privileges were dropped successfully
- Failure to deallocate data
- Failure to provide confidentiality for stored data
- Guessed or visible temporary file
- Improper cleanup on thrown exception
- Improper error handling

- Improper temp file opening
- Incorrect block delimitation
- Misinterpreted function return value
- Missing parameter
- Omitted break statement
- Passing mutable objects to an untrusted method
- Symbolic name not mapping to correct object
- Truncation error
- Undefined Behavior
- Uninitialized Variable
- Unintentional pointer scaling
- Use of sizeof() on a pointer type
- Using the wrong operator
- Business logic flaw

Input and Output Validation

Description

Input validation is the process of ensuring that the user-supplied content contains only expected information. Input validation covers a wide assortment of potential exploitation, but requires caution. Failing to properly validate external input may allow execution of unintended functionality, and often "arbitrary code execution".

Examples

- Buffer Overflow
- Format String
- Improper Data Validation
- Log Forging
- Missing XML Validation
- Process Control
- String Termination Error
- Unchecked Return Value: Missing Check against Null
- Unsafe JNI
- Unsafe Reflection
- Validation performed in client

- Unvalidated redirects and forwards

Logging and Auditing Vulnerability

Description

Logging and auditing are common system and security functions aiding in system management, event identification, and event reconstruction. This vulnerability class deals with issues that either aid in an attack or increase the likelihood of its success due to logging and auditing.

Examples

- Addition of data-structure sentinel
- Log Corruption
- Lack of Regular Log Review
- Information Leakage
- Log Forging
- Log injection
- Poor Logging Practice
- Cross-site scripting via HTML log-viewers

Password Management Vulnerability

Description

Passwords are the most commonly used form of authentication. This class of vulnerabilities deals with mistakes in handling passwords that may allow an attacker to obtain or guess them.

Examples

- Allowing password aging
- Empty String Password
- Hard-Coded Password
- Not allowing password aging
- Password Management: Hardcoded Password
- Password Management: Weak Cryptography
- Password Plaintext Storage
- Password in Configuration File
- Using password systems

Path Vulnerability

Description

"This category is for tagging path issues that allow attackers to access files that are not intended to be accessed. Generally, this is due to dynamically construction of a file path using unvalidated user input" (OWASP page).

Examples

- Path Traversal Attack
- Relative Path Traversal Attack
- Virtual Files Attack
- Path Equivalence Attack
- Link Following Attack
- Virtual Files Attack

Protocol Errors

Description

Protocols are rules of communication. This vulnerability class deals with the security issues introduced during protocol design.

Examples

- Failure to add integrity check value
- Failure to check for certificate revocation
- Failure to check integrity check value
- Failure to encrypt data
- Failure to follow chain of trust in certificate validation
- Failure to protect stored data from modification
- Failure to validate certificate expiration
- Failure to validate host-specific certificate data
- Key exchange without entity authentication
- Storing passwords in a recoverable format
- Trusting self-reported DNS name
- Trusting self-reported IP address
- Use of hard-coded password
- Insufficient transport layer protection
- Use of weak SSL/TLS protocols
- SSL/TLS key exchange without authentication

- SSL/TLS weak key exchange
- Low SSL/TLS cipher strength

Potential Impact

Compromise of security protocols such as TLS

Range and Type Error Vulnerability

Description

Range and type errors are common programming mistakes. This vulnerability class covers the various types of errors that have potential security consequences.

Examples

- Access control enforced by presentation layer
- Buffer Overflow
- Buffer underwrite
- Comparing classes by name
- Deserialization of untrusted data
- Doubly freeing memory
- Failure to account for default case in switch
- Format String
- Heap overflow
- Illegal Pointer Value
- Improper string length checking
- Integer coercion error
- Integer overflow
- Invoking untrusted mobile code
- Log Forging
- Log injection
- Miscalculated null termination
- Null Dereference
- Often Misused: String Management
- Reflection injection
- Sign extension error
- Signed to unsigned conversion error

- Stack overflow
- Truncation error
- Trust Boundary Violation
- Unchecked array indexing
- Unsigned to signed conversion error
- Using freed memory
- Validation performed in client
- Wrap-around error
- Cardinality incorrect
- Value integrity modification
- Sequencing or timing error

Sensitive Data Protection Vulnerability

Description

"This category is for tagging vulnerabilities that lead to insecure protection of sensitive data. The protection referred here includes confidentiality and integrity of data during its whole lifecycles, including storage and transmission.

"Please note that this category is intended to be different from access control problems, although they both fail to protect data appropriately. Normally, the goal of access control is to grant data access to some users but not others. In this category, we are instead concerned about protection for sensitive data that are not intended to be revealed to or modified by any application users. Examples of this kind of sensitive data can be cryptographic keys, passwords, security tokens or any information that an application relies on for critical decisions" (OWASP page).

Examples

- Information leakage results from insufficient memory clean-up
- Inappropriate protection of cryptographic keys
- Clear-text Passwords in configuration files
- Lack of integrity protection for stored user data
- Hard-Coded Password
- Heap Inspection
- Information Leakage
- Password Management: Hardcoded Password
- Password Plaintext Storage
- Privacy Violation

Session Management Vulnerability

Description

Session management is the way with which a client and server connect, maintain, and close a connection. Primarily an issue with Web interfaces, this class covers vulnerabilities resulting from poor session management.

Examples

- Applications should NOT use as variables any user personal information (user name, password, home address, etc.).
- Highly protected applications should not implement mechanisms that make automated requests to prevent session timeouts.
- Highly protected applications should not implement "remember me" functionality.
- Highly protected applications should not use URL rewriting to maintain state when cookies are turned off on the client.
- Applications should NOT use session identifiers for encrypted HTTPS transport that have once been used over HTTP.
- Insufficient Session-ID Length
- Session Fixation
- Cross site request forgery
- Cookie attributes not set securely (e.g. domain, secure and HTTP only)
- Overly long session timeout

Concurrency, Synchronization and Timing Vulnerability

Description

Concurrency, synchronization and timing deals with the order of events in a complex computing environment. This vulnerability class deals with timing issues that affect security, most often dealing with multiple processes or threads which share some common resource (file, memory, etc.).

Examples

- Capture-replay
- Covert timing channel
- Failure to drop privileges when reasonable
- Failure to follow guideline/specification
- File Access Race Condition: TOCTOU
- Member Field Race Condition
- Mutable object returned

- Overflow of static internal buffer
- Race Conditions
- Reflection attack in an auth protocol
- State synchronization error
- Unsafe function call from a signal handler

Insufficient Safeguards for Mobile Code

Description

Mobile code consists of programming instructions transferred from client to server that execute on the client machine without the user explicitly initiating that execution. Allowing mobile code generally increases attack surface. This section includes issues that permit the execution of unsafe mobile code.

Examples

- VBScript, JavaScript and Java sandbox container flaws
- Insufficient scripting controls
- Insufficient code authentication

Buffer Overflow

Description

Software used to implement an ICS could be vulnerable to buffer overflows; adversaries could exploit these to perform various attacks. (SP 800-82)

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold, or when a program attempts to put data in a memory area outside of the boundaries of a buffer. The simplest type of error, and the most common cause of buffer overflows, is the "classic" case in which the program copies the buffer without checking its length at all. Other variants exist, but the existence of a classic overflow strongly suggests that the programmer is not considering even the most basic of security protections. (CWE)

Examples

- CVE-1999-0046 - buffer overflow in local program using long environment variable
- CVE-2000-1094 - buffer overflow using command with long argument
- CVE-2001-0191 - By replacing a valid cookie value with an extremely long string of characters, an attacker may overflow the application's buffers.
- CVE-2002-1337 - buffer overflow in comment characters, when product increments a counter for a ">" but does not decrement for "<"
- CVE-2003-0595 - By replacing a valid cookie value with an extremely long string of characters, an attacker may overflow the application's buffers (CWE).

Mishandling of Undefined, Poorly Defined, or "Illegal" Conditions

Description

Some ICS implementations are vulnerable to packets that are malformed or contain illegal or otherwise unexpected field values (SP 800-82)

Use of Insecure Protocols

Description

Protocols are expected patterns of behavior that allow communition among computing resources. This section deals with the use of protocols for which security was not sufficiently considered during the development process.

Examples

- Distributed Network Protocol (DNP) 3.0, Modbus, Profibus, and other protocols are common across several industries and protocol information is freely available. These protocols often have few or no security capabilities built in (SP 800-82).
- Use of clear text protocols such as FTP and Telnet
- Use of proprietary protocols lacking security features

Potential Impact

Weaknesses that Affect Files and Directories

Description

Weaknesses in this category affect file or directory resources (CWE).

Examples

- UNIX Path Link Problems
- Windows Path Link Problems
- Windows Virtual File Problems
- Mac Virtual File Problems
- Failure to Resolve Case Sensitivity
- Path Traversal
- Failure to Change Working Directory in chroot Jail
- Often Misused: Path Manipulation
- Password in Configuration File
- Improper Ownership Management
- Improper Resolution of Path Equivalence
- Information Leak Through Server Log Files

- Files or Directories Accessible to External Parties
- Improper Link Resolution Before File Access ('Link Following')
- Improper Handling of Windows Device Names
- Improper Sanitization of Directives in Statically Saved Code ('Static Code Injection')

C.3.2 API Usage and Implementation

API Abuse

Description

"An API is a contract between a caller and a callee. The most common forms of API abuse are caused by the caller failing to honor its end of this contract" (OWASP page).

Examples

"For example, if a program fails to call chdir() after calling chroot(), it violates the contract that specifies how to change the active root directory in a secure fashion. Another good example of library abuse is expecting the callee to return trustworthy DNS information to the caller. In this case, the caller abuses the callee API by making certain assumptions about its behavior (that the return value can be used for authentication purposes). One can also violate the caller-callee contract from the other side. For example, if a coder subclasses SecureRandom and returns a non-random value, the contract is violated" (OWASP page).

- Dangerous Function
- Directory Restriction Error
- Failure to follow guideline/specification
- Heap Inspection
- Ignored function return value
- Object Model Violation: Just One of equals() and hashCode() Defined
- Often Misused: Authentication
- Often Misused: Exception Handling
- Often Misused: File System
- Often Misused: Privilege Management
- Often Misused: String Management

Use of Dangerous API

Description

Use of an application programming interface (API) which is inherently dangerous or fraught with error.

Examples

- Dangerous Function such as the C function gets()
- Directory Restriction Error
- Failure to follow guideline/specification
- Heap Inspection
- Insecure Temporary File
- Object Model Violation: Just One of equals() and hashCode() Defined
- Often Misused: Exception Handling
- Often Misused: File System
- Often Misused: Privilege Management
- Often Misused: String Management
- Unsafe function call from a signal handler
- Use of Obsolete Methods

C.4 PLATFORM VULNERABILITIES

Platforms are defined as the software and hardware units, or systems of software and hardware, that are used to deliver software based services.

The platform comprises the software, the operating system used to support that software, and the physical hardware. Vulnerabilities arise in this part of the Smart Grid network due to the complexities of architecting, configuring, and managing the platform itself. Platform areas identified as being vulnerable to risk include the security architecture and design, inadequate malware protection against malicious software attacks, software vulnerabilities due to late or nonexistent software patches from software vendors, an overabundance of file transfer services running, and insufficient alerts from log management servers and systems.

C.4.1 Design

Inadequate Security Architecture and Design

Description

This is more of a cause of vulnerabilities than a vulnerability in itself. Would it be appropriate to leave it out?

C.4.2 Implementation

Inadequate Malware Protection

Description

Malicious software can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data. Malware protection software, such as antivirus software, is needed to prevent systems from being infected by malicious software (SP 800-82).

Examples

- Malware protection software not installed
- Malware protection software or definitions not current
- Malware protection software implemented without exhaustive testing

Installed Security Capabilities Not Enabled by Default

Description

Security capabilities must obviously be turned on to be useful. There are many examples of operating systems (particularly Microsoft operating systems pre-Vista) where protections such as firewalls are configured but not enabled out-of-the-box. If protections are not enabled, the system may be unexpectedly vulnerable to attacks. In addition, if the administrator does not realize that protections are disabled, the system may continue in an unprotected state for some time until the omission is noticed.

Absent or Deficient Equipment Implementation Guidelines

Description

Unclear implementation guidelines can lead to unexpected behavior.

A system will need to be configured correctly if it is to provide the desired security properties. This applies to both hardware and software configuration. Different inputs and outputs, both logical and physical, will have different security properties, and an interface that is supposed to be for internal use may be more vulnerable than an interface that is supposed to be for external use. As such, guidelines for installers, operators and managers must be clear about the security properties expected of the system and how the system is to be implemented and configured in order to obtain those properties.

C.4.3 Operational

Lack of Prompt Security Patches from Software Vendors

Description

Software contains bugs and vulnerabilities. When a vulnerability is disclosed there will be a race between hackers and patchers to exploit or close the loophole. The security of the system using the software therefore depends crucially on vendors' ability to provide patches in a timely manner, and on administrators' ability to implement those patches. As zero-day exploits become more widespread, administrators may be faced with the alternatives of taking a system offline or leaving it vulnerable.

Examples

Potential Impact

Unneeded Services Running

Description

Many OSes are shipped and installed with a number of services running by default: for example, in the Unix case, an installation may automatically offer telnet, ftp, and http servers. Every service that runs is a security risk, partly because intended use of the service may provide access to system assets, and partly because the implementation may contain exploitable bugs. Services should only run if needed and an unneeded service is a vulnerability with no benefit.

Examples

Potential Impact

Insufficient Log Management

Description

Events from all devices should be logged to a central log management server. Alerts should be configured according to the criticality of the event or a correlation of certain events. For instance, when the tamper detection mechanism on a device is triggered, an alert should be raised to the appropriate personnel. When X number of meters are issued a remote power disconnect command within a certain time frame, alerts should also be sent.

Examples

- Inadequate network security architecture (800-82 3-8)
- Poorly configured security equipment (SP 800-82 3-8)
- Inadequate firewall and router logs (800-82 3-11)
- No security monitoring on the network (800-82 3-11)
- Critical monitoring and control paths are not identified (800-82 3-12)

Potential Impact

- Failure to detect critical events
- Removal of Forensic Evidence
- Log Wipes

Inadequate Anomaly Tracking

Description

Alerts and logging are two useful techniques for detecting and mitigating the risk of anomalous events, but can themselves present security risks or become vulnerabilities if not done thoughtfully. Appropriate reaction to an event will vary according to the criticality of the event

or a correlation of certain events, and may also need to be logged. A central logging facility may also be necessary for correlating events. Appropriate event reactions could include automatic paging of relevant personnel in the event of persistent tamper messages or requiring positive acknowledgement to indicate supervisory approval before executing a potentially disruptive command such as simultaneously disconnecting many loads from the electrical grid or granting control access rights to hundreds of users.

C.5 NETWORK

Networks are defined by connections between multiple locations, organizational units and are comprised of many differing devices using similar protocols and procedures to facilitate a secure exchange of information. Vulnerabilities and risks occur within smart grid networks when policy management and procedures as they relate to the data exchanged do not conform to required standards and compliance polices.

Network areas identified as being susceptible to risk and with policy and compliance impacts are: data integrity, security, protocol encryption, authentication, and device hardware.

Inadequate Integrity Checking

Description

The integrity of message protocol and message data is should be verified before routing or processing. Devices receiving data that does not conform to the protocol or message standard should not act on such traffic (e.g. forwarding to another device or changing its own internal state) as though it were correctly received.

This should be done before any application attempts to use the data for internal processes or routing to another device. Additionally, special security devices acting as application level firewalls should be used to logical bounds checking, such as preventing the shutdown of all power across an entire NAN.

Most functions of the smart grid, such as Demand Response, Load Shedding, AMR, ToU, and Distribution Automation require that data confidentiality and/or data integrity be maintained to ensure grid reliability, prevent fraud, and for reliable auditing. Failure to apply integrity and confidentiality services where needed can result in vulnerabilities such as exposure of sensitive customer data, unauthorized modification of telemetry data, transaction replay, and audit manipulation.

Examples

- Lack of integrity checking for communications (800-82 3-12)
- Failure to detect and block malicious traffic in valid communication channels
- Inadequate network security architecture (800-82 3-8)
- Poorly configured security equipment (800-82 3-8)
- No security monitoring on the network (800-82 3-11)

Potential Impact

- Compromise of smart device, head node, or utility management servers.
- Buffer Overflows
- Covert Channels
- MitM
- DoS / DDoS

Inadequate Network Segregation

Description

Network architecture does a poor job at defining security zones and controlling traffic between security zones. Often this is considered a flat network that allows traffic from any portion of the network to communicate with any other portion of the network. Smart Grid examples might be failure to install a firewall to control traffic between a head node and the utility company or failure to prevent traffic from one NAN to another NAN.

Examples

- Failure to Define Security Zones
- Failure to Control traffic between Security Zones
- Inadequate Firewall Ruleset
- Firewalls nonexistent or improperly configured (800-82 3-10)
- Improperly Configured VLAN
- Inadequate access controls applied (800-82 3-8)
- Inadequate network security architecture (800-82 3-8)
- Poorly configured security equipment (800-82 3-8)
- Control networks used for non-control traffic (800-82 3-10)
- Control network services not within the control network (800-82 3-10)
- Critical monitoring and control paths are not identified (800-82 3-12)

Potential Impact

- Direct compromise of any portion of the network from any other portion of fhe network
- Compromise of the Utility network from a NAN network
- VLAN Hopping
- Network Mapping
- Service/Device Exploit
- Covert Channels

- Back Doors
- Worms and other malicious software

Inappropriate Protocol Selection

Description

It is important to note that the use of encryption is not always the appropriate choice. A full understanding of the information management capabilities that are lost through the use of encryption should be completed before encrypting unnecessarily

Use of unencrypted network protocols or weakly encrypted network protocols exposes authentication keys and data payload. This may allow attackers to obtain credentials to access other devices in the network and decrypt encrypted traffic using those same keys. The use of clear text protocols may also permit attackers to perform session hijacking and man-in-the-middle attacks allowing the attacker to manipulate the data being passed between devices.

Examples

- Standard, well-documented communication protocols are used in plain text in a manner which creates a vulnerability.(800-82 3-12)
- Inadequate data protection between clients and access points (800-82 3-13)

Potential Impact

- Compromise of all authentication and payload data being passed
- Session Hijacking
- Authentication Sniffing
- MitM Attacks
- Session Injection

Weaknesses in Authentication Process or Authentication Keys

Description

Authentication mechanism does not sufficiently authenticate devices or exposes authentication keys to attack.

Examples

- Inappropriate Lifespan for Authentication Credentials/Keys
- Inadequate Key Diversity
- Authentication of users, data or devices is substandard or nonexistent (800-82 3-12)
- Insecure key storage
- Insecure key exchange
- Insufficient account lockout

- Inadequate authentication between clients and access points (800-82 3-13)
- Inadequate data protection between clients and access points (800-82 3-13)

Potential Impact

- DoS / DDoS
- MitM
- Session Hijacking
- Authentication Sniffing
- Session Injection

Insufficient Redundancy

Description

Architecture does not provide for sufficient redundancy exposing the system to intentional or unintentional denial of service.

Examples

- Lack of redundancy for critical networks (800-82 3-9)

Potential Impact

- Denial of Service (DoS / DDoS)

Physical Access to the Device

Description

Access to physical hardware may lead to a number of hardware attacks that can lead to the compromise of all devices and networks. Physical access to smart grid devices should be limited according to the criticality or sensitivity of the device. Ensuring the physical security of smart grid elements, such as by physically locking them in some secure building or container is preferred where practical. In other circumstances, tamper resistance, tamper detection, and intrusion detection and alerting are among the many techniques that can complement physically securing devices.

Examples

- Unsecured physical ports
- Inadequate physical protection of network equipment (800-82 3-9)
- Loss of environmental control (800-82 3-9)
- Non-critical personnel have access to equipment and network connections (800-82 3-9)

Potential Impact

- Malicious Configurations

- MitM
- EEPROM Dumping
- Micro Controller Dumping
- Bus Snooping
- Key Extraction

REFERENCES

NIST Special Publication 800-82, *Guide to Industrial Control Systems Security*
http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

Open Web Application Security Project (OWASP)
http://www.owasp.org/index.php/Category:Vulnerability

NERC Critical Infrastructure Protection Standards
http://www.nerc.com/

APPENDIX D
BOTTOM-UP SECURITY ANALYSIS OF THE SMART GRID

D.1 Scope of This Effort

This effort, a subgroup of the SGIP-CSWG, is performing a bottom-up analysis of cyber security issues in the evolving Smart Grid. The goal is to identify specific protocols, interfaces, applications, best practices, etc. that could and should be developed to solve specific Smart Grid cyber security problems. The approach taken herein is **bottom-up**; that is, to identify some specific problems and issues that need to be addressed, but not to perform a comprehensive gap analysis that covers all issues. This effort intends to complement the top-down efforts being followed elsewhere in the SGIP-CSWG. By proceeding with a bottom-up analysis, our hope is to more quickly identify fruitful areas for solution development, while leaving comprehensive gap analysis to other efforts of the SGIP-CSWG, and providing an independent completeness check for top-down gap analyses. This effort is proceeding simultaneously in several phases.

First, we have captured a number of **evident and specific security problems** in the Smart Grid that are amenable to and should have open and interoperable solutions, but are not obviously solved by existing standards, de facto standards, or best practices. This list includes only cyber security problems that have some specific relevance to or uniqueness in the smart grid. Thus we do not list general cyber security problems such as poor software engineering practices, key management, etc. unless these problems have some unique twist when considered in the context of the smart grid. We are continuing to add to this list of problems as we come across problems not yet documented.

In conjunction with developing the list of specific problems, we have developed a separate list of more **abstract security issues** that are not as specific as the problems in the first list, but are nevertheless of significant importance. Considering these issues in specific contexts can reveal specific problems.

Next, drawing in part from the specific problems and abstract issues cataloged in the first two lists, we are developing a third list of cyber security **design considerations** for smart grid systems. These design considerations discuss important cyber security issues that arise in the design, deployment, and use of smart grid systems, and should be considered by system designers, implementers, purchasers, integrators, and users of smart grid technologies. In discussing the relative merits of different technologies or solutions to problems, these design considerations stop short of recommending specific solutions or even requirements. Our intention is to highlight important issues that can serve as a means of identifying and formulating requirements and high-level designs for key protocols and interfaces that are missing and need to be developed.

D.2 Device Class Definitions

The following device definitions are based on a classified NERC and DHS publication. The use of the definitions has been cleared, but the specific document reference cannot be given as it is classified in its own right. The issues that are discussed apply to these mentioned device classes.

Remote Terminal Units (RTUs) – In a SCADA system, an RTU is a device installed at a remote location to collect and code data in a transmittable format back to a central station or master. RTUs typically connect to input and output channels. Input channels are equipped to handle metering information and sensing changes. Output channels are equipped for control or alarms. Continuous communication to an RTU is accomplished through an internally-controlled or externally-provided serial or network connection. Typical environments can also include dial-up connections where continuous monitoring is not required.

Programmable Logic Controllers (PLCs) / Intelligent Electronic Devices (IEDs) / Relays – Most electric utilities have separate Distributed Control Systems (DCS) and Relay Protection Systems for their power plants and substation control systems. In a substation environment PLCs and IEDs are used to protect transformers and customer equipment when a specific undesirable event occurs on the transmission or distribution system. In power plants, this type of equipment is used to protect associated generating equipment from internal and external system failures. Current technology in electric power distribution automation also includes IEDs on the feeder, outside the substation fence. The simplest of these devices perform such functions as local control of switched capacitor banks (over 100,000 of these are deployed in North America), feeder switching devices including remotely-operable switches, switch operators, sectionalizers and reclosers (automatically-reclosing circuit breakers). In addition to these relatively simple devices, feeder automation also includes DCSs, some of which perform automatic feeder reconfiguration (switching) to isolate and reroute power in the event of a fault on the circuit. These systems can be very sophisticated, involving pure, peer-oriented distributed logic and traveling autonomous software agents. Commercial application of these latter systems numbers in the many thousands of units. With the emergence of the Smart Grid, new classes of IEDs are being developed to manage a wide variety of alternative energy and energy storage devices.

Smart Meters – A type of advanced meter that identifies consumption in more detail than a conventional meter. Communication to this type of meter is typically accomplished using the internet, wireless networks, local power lines, or fiber back to the local utility provider.

Specialized communication hardware – Internally-controlled communication networks such as microwave, fiber optic, or RF-based technologies are the platforms utilized by the electrical sector to connect remote devices to central stations or masters. Examples can include routers, gateways, switches, access points, and modems.

D.3 Evident and Specific Cyber Security Problems

This section documents specific cyber security problems in the smart grid, as much as possible by describing actual field cases that explain exactly the operational, system, and device issues. The problems listed herein are intentionally *not* ordered or categorized in any particular way.

D.3.1 Openness and Accessibility of Smart Grid Standards

Many standards relevant to the smart grid are published by organizations such as IEEE, ANSI, IEC, etc. While the standards published by these organizations are open, they are not nearly as freely accessible as the IETF standards that define the Internet and World Wide Web. Many of the smart grid standards must be purchased, and the cost for a single standard can range into thousands of dollars. In many cases the license accompanying a standard restricts its use to a single individual, and in some cases electronic copies of the standard are protected by Digital Rights Management technology that locks the copy to a specific computer (e.g. ANSI standards).

Designing algorithms and protocols that operate correctly and are free of undiscovered flaws is difficult at best. There is general agreement in the security community that openly published and time-tested algorithms and protocols are less likely to contain security flaws than secretly developed ones because their publication enables scrutiny by the entire community. Limitations to standards accessibility, in the form of purchase costs and restrictive licenses, may similarly discourage inspection and review by parties without strong motivation and financial backing, and may increase the risk that smart grid standards contain security vulnerabilities.
The above barrier to evaluation and use of standards has been discussed at several stages during the process of developing the NIST Smart Grid Framework/Roadmap and remain on the agenda of NIST-related efforts. They are also addressed in the IEEE-USA National Energy Policy Recommendations and in the (forthcoming) background statement that accompanies those recommendations.
Factors contributing to the issue include:

- The various governance and funding models of the SDOs
- For international SDOs, the governance and funding models of their affiliated U.S. National Committees. For example, for IEC the national committees determine distribution policies within their countries.
- For some SDOs the lack of provisions in their practices and funding models for standards of high public visibility and national importance.
- The general avoidance by the Federal government of a role in funding SDOs and their U.S. participants (as is often done by governments of other countries), even for standards of particular interest to the government.
- A legally murky situation regarding the public right to copies of standards that become integrated in some way into law or regulation.

D.3.2 Authenticating and Authorizing Users to Substation IEDs

The problem is how to authenticate and authorize users (maintenance personnel) to Intelligent Electronic Devices (IEDs) in substations in such a way that access is specific to a user, authentication information (e.g. password) is specific to each user (i.e. not shared between users), and control of authentication and authorization can be centrally managed across all IEDs in the substation and across all substations belonging to the utility and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

Currently many substation IEDs have a notion of “role” but no notion of “user”. Passwords are stored locally on the device and several different passwords allow different authorization levels. These role passwords are shared amongst all users of the device with the role in question, possibly including non-utility employees such as contractors and vendors. Furthermore, due to the number of devices, these passwords are often the same across all devices in the utility, and seldom changed.

The device may be accessed locally in the sense that the user is physically present in the substation and accesses the IED from a front panel connection or wired network connection, or

possibly wireless. The device may also be accessed remotely over a low-speed (dialup) or high-speed (network) connection from a different physical location.

Substations generally have some sort of connectivity to the control center that might be used to distribute authentication information and collect audit logs, but this connectivity may be as slow as 1200 baud. Performing an authentication protocol such as RADIUS or LDAP over this connection is probably not desirable. Furthermore, reliance on central authentication servers is unwise, since authentication should continue to apply for personnel accessing devices locally in the substation when control center communications are down.

A provision to ensure that necessary access is available in emergency situations may be important, even if it means bypassing normal access control, but with an audit trail.

D.3.3 Authenticating and Authorizing Users to Outdoor Field Equipment

Some newer pole-top and other outdoor field equipment supports 802.11 or Bluetooth for near-local user access from a maintenance truck. The problem is how to authenticate and authorize users (maintenance personnel) to such devices in such a way that access is specific to a user (person), authentication information (e.g. password) is specific to each user (not shared between users), and control of authentication and authorization can be centrally managed across the utility and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

Pole-top and other outdoor field equipment may not have connectivity to the control center. Access will usually be local via wired connections, or near-local via short-range radio, although some devices may support true remote access.

Strong Authentication and authorization measures are preferable, and in cases where there is documented exception to this due to legacy and computing constrained devices, compensating controls should be given due consideration. For example in many utility organizations, very strong operational control and workflow prioritization is in place, such that all access to field equipment is scheduled, logged, and supervised. In the general sense, the operations department typically knows exactly who is at any given field location at all times. In addition, switchgear and or other protective equipment generally have tamper detection on doors as well as connection logging and reporting such that any unexpected or unauthorized access can be reported immediately over communications.

D.3.4 Authenticating and Authorizing Maintenance Personnel to Meters

Like IED equipment in substations, current smart meter deployments use passwords in meters that are not associated with users. Passwords are shared between users and the same password is typically used across the entire meter deployment. The problem is how to authenticate and authorize users who are maintenance personnel to meters in such a way that access is specific to a user, authentication information (e.g. password) is specific to each user (i.e. not shared between users), and control of authentication and authorization can be centrally managed and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

Access may be local through the optical port of a meter, or remote through the AMI infrastructure, or remote through the HAN gateway.
Meters generally have some sort of connectivity to an AMI head end, but this connectivity may be as slow as 1200 baud, or lower (e.g. some power line carrier devices have data rates measured in millibaud). This connectivity cannot be assumed to be present in a maintenance scenario.

D.3.5 Authenticating and Authorizing Consumers to Meters

Where meters act as home area network gateways for providing energy information to consumers and/or control for demand response programs, will consumers be authenticated to meters? If so, authorization would likely be highly limited. What would the roles be? Authorization and access levels need to be carefully considered, i.e., a consumer capable of supplying energy to the power grid may have different access requirements than one who does not.

D.3.6 Authenticating Meters to/from AMI Head Ends

It is important for a meter to authenticate any communication from an AMI head end, in order to ensure that an adversary cannot issue control commands to the meter, update firmware, etc. It is important for an AMI head end to authenticate the meter, since usage information retrieved from the meter will be used for billing, and commands must be assured of delivery to the correct meter.

As utilities merge and service territories change, a utility will eventually end up with a collection of smart meters from different vendors. Meter to/from AMI head end authentication should be interoperable to ensure that authentication and authorization information need not be updated separately on different vendor's AMI systems.

D.3.7 Authenticating HAN Devices to/from HAN Gateways

Demand response HAN devices must be securely authenticated to the HAN gateway and vice versa. It is important for a HAN device to authenticate any demand-response commands from the DR head end to order to prevent control by an adversary. Without such authentication, coordinated falsification of control commands across many HAN devices and/or at rapid rates could lead to grid stability problems. It is important that the DR head end authenticate the HAN device both to ensure that commands are delivered to the correct device, and that responses from that device are not forged.

Interoperability of authentication is essential in order to ensure competition that will lead to low cost consumer devices. This authentication process must be simple and fairly automatic since to some degree it will be utilized by consumers who buy/rent HAN devices and install them. HAN devices obtained by the consumer from the utility may be pre-provisioned with authentication information. HAN devices obtained by the consumer from retail stores may require provisioning through an Internet connection or may receive their provisioning through the HAN gateway.

Should a HAN device fail to authenticate, it will presumably be unable to respond to demand response signals. It should not be possible for a broad DOS attack to cause a large number of HAN devices to fail to authenticate and thereby not respond to a DR event.

D.3.8 Authenticating Meters to/from AMI Networks

Meters and AMI networks are more susceptible to wide-spread compromise and DoS (Denial of Service) attacks if no authentication and access control is provided in AMI access networks such as NANs and HANs. The vulnerability exists even if the rest of the AMI network is secured and encryption and integrity are provided by an AMI application protocol. Network access authentication tied with access control in the AMI access networks can mitigate the threat by ensuring only authenticated and authorized entities can gain access to the NANs or HANs. In mesh networks, this "gatekeeper" functionality must be enforced at each node. The network access authentication must be able to provide mutual authentication between a meter and an access control enforcement point. A trust relationship between the meter and the enforcement point may be dynamically established using a trusted third-party such as an authentication server. Providing network access authentication for mesh networks can be more challenging than non-mesh networks due to difference in trust models between mesh networks and non-mesh networks. One trust model for mesh networks is based on dynamically created hop-by-hop chain of trust between adjacent mesh nodes on the path between a leaf mesh node and the gateway to the AMI network where access control is performed on each intermediate mesh node and the gateway. Another trust model for mesh networks is end-to-end trust between a leaf mesh node and the gateway where intermediate mesh nodes are considered untrusted to the leaf node and a secured tunnel may be created between each leaf node and the gateway. These two trust models can co-exist in the same mesh network. When two or more inter-connected mesh networks are operated in different trust models, end-to-end security across these mesh networks is the only way to provide data security for applications running across the mesh networks. There has been some research done in the area of wireless sensor networks that is relevant to mesh networks. For instance, there are scalable key predistribution schemes [LiuNing] that are resistant to node capture and operate well on devices with limited computational capabilities.

D.3.9 Securing Serial SCADA Communications

Many substations and distribution communication systems still employ slow serial links for various purposes including SCADA communications with control centers and distribution field equipment. Furthermore, many of the serial protocols currently in use do not offer any mechanism to protect the integrity or confidentiality of messages, i.e., messages are transmitted in clear text form. Solutions that simply wrap a serial link message into protocols like SSL or IPSEC over PPP will suffer from the overhead imposed by such protocols (both in message payload size and computational requirements) and would unduly impact latency and bandwidth of communications on such connections. A solution is needed to address the security and bandwidth constraints of this environment.

D.3.10 Securing Engineering Dialup Access

Dialup is often used for engineering access to substations. Broadband is often unavailable at many remote substation locations. Security is limited to modem callback and passwords in the answering modem and/or device connected to the modem. Passwords are not user-specific and are seldom changed. A solution is needed that gives modern levels of security while providing for individual user attribution of both authentication and authorization.

D.3.11 Secure End-to-End Meter to Head End Communication

Secure end-to-end communications protocols such as TLS ensure that confidentiality and integrity of communications is preserved regardless of intermediate hops. End-to-end security between meters and AMI head ends is desirable, and even between HAN devices and Demand Response control services.

D.3.12 Access Logs for IEDs

Not all IEDs create access logs. Due to limited bandwidth to substations, even where access logs are kept, they are often stranded in the substation. In order for a proper Security Event Management paradigm to occur these logs will need to become centralized and standardized so that other security tools can analyze their data. This is important in order to detect malicious actions by insiders as well as systems deeply penetrated systems by attackers that might have subtle mis-configurations as part of a broader attack. A solution is needed that can operate within the context of bandwidth limitations found in many substations as well as the massively distributed nature of power grid infrastructure.

D.3.13 Remote Attestation of Meters

Remote attestation provides a means to determine whether a remote field unit has an expected and approved configuration. For meters, this means the meter is running correct version and un-tampered firmware with appropriate settings, and has *always* been running un-tampered firmware. Remote attestation is particularly important for meters given the easy physical accessibility of meters to attackers.

D.3.14 Protection of Routing Protocols in AMI Layer 2/3 Networks

In the AMI space, there is increasing likelihood that mesh routing protocols will be used on wireless links. Wireless suffers from several well-known and often easily exploitable attacks partly due to the lack of control to the physical medium (the radio waves). Modern mechanisms like 802.11i have worked to close some of these holes for standard wireless deployments. However, wireless mesh technology potentially opens the door to some new attacks in the form of route injection, node impersonation, L2/L3/L4 traffic injection, traffic modification, etc. Most current on-demand and link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, primarily because of the distributed nature of the system itself. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without routing security, attacks such as eavesdropping, impersonation, man-in-the-middle, and denial-of-service could be easily mounted on AMI traffic.

D.3.15 Key Management for Meters

Where meters contain cryptographic keys for authentication, encryption, or other cryptographic operations, a key management scheme must provide for adequate protection of cryptographic materials as well as sufficient key diversity. That is, a meter, collector, or other power system device should not be subject to a break-once break-everywhere scenario due to one shared secret being used across the entire infrastructure. Each device should have unique credentials and key material such that compromise of one device does not impact other deployed devices. The key management system must also support an appropriate lifecycle of periodic re-keying and revocation.

There are existing cases of large deployed meter bases using the same symmetric key across all meters, and even in different States. In order to share network services, adjacent utilities may even share and deploy that key information throughout both utility AMI networks. Compromising a meter in one network could compromise all meters and collectors in both networks.

D.3.16 Protection of Dial-up Meters

Reusing older, time-proven technologies such as dial-up modems to connect to collectors or meters without understanding the subtle differences in application may provide loss of service or worse. Dial-up technology using plain-old telephone service (POTS) has been a preferred method for connecting to network gear, particularly where a modem-bank providing 24, 48 or even 96 modems/phone-numbers and other anti-attack intelligence is used. However, dialing into a collector or modem and connecting, even without a password, can deprive that ability to the utility, effectively denying service. Consider a utility which, for the sake of manageability places all their collectors or modems on phone numbers in a particular prefix. Every collector then can be hit by calling 202-555-WXYZ.

D.3.17 Outsourced WAN Links

Many utilities are leveraging existing communications infrastructure from telecommunications companies to provide connectivity between generation plants and control centers, between substations and control centers (particularly SCADA), and increasingly between pole-top AMI collectors and AMI head end systems, and pole-top distribution automation equipment and distribution management systems.

Due to the highly distributed nature of AMI, it is more likely that an AMI WAN link will be over a relatively low bandwidth medium such as cellular band wireless (e.g., EVDO, GPRS) or radio networks like FlexNet. The link layer security supported by these networks varies greatly. Later versions of WiMax can utilize EAP for authentication, but NIST SP800-127 provides a number of recommendations and cautions about WiMax authentication. With cellular protocols, the AirCards used by the collector modems are no different than the ones used for laptops. They connect to a wireless cloud typically shared by all local wireless users, with no point-to-point encryption, and no restrictions on whom in the wireless cloud can connect to the collector modem's interface. From the wireless, connectivity to the head end system is usually over the Internet, sometimes (hopefully always) using a VPN connection. Given the proliferation of botnets, it is not far-fetched to imagine enough wireless users to be compromised and launch a denial of service via a collector modem.

Regardless of the strength of any link layer security implemented by the communications service provider, without end-to-end VPN security, the traffic remains accessible to insiders at the service provider. This can permit legitimate access such as lawful intercept, but also can allow unscrupulous insiders at the service provider access to the traffic.
Additionally, like the mesh wireless portion, cellular networks are subject to intentional and unintentional interference and congestion. Cellular networks were significantly disrupted in Manhattan during the 9/11 attacks by congestion and rendered mostly unusable to first responders. Similar congestion events could disrupt utility communications relying on commercial WAN links.

D.3.18 Insecure Firmware Updates

The ability to perform firmware updates on meters in the field allows for the evolution of applications and the introduction of patches without expensive physical visits to equipment. However, it is critical to assure that firmware update mechanisms are not used to install malware. This can be addressed by a series of measures that provide a degree of defense in depth. First, measures can be taken to assure that software is created without flaws such as buffer overflows that can enable protection measures to be circumvented. Techniques for programming languages and static analysis provide a foundation for such measures. Second, principals attempting updates must be properly authenticated and authorized for this function at a suitable enforcement point such as on the meter being updated. Third, software can be signed in a way that it can be checked for integrity at any time. Fourth, remote attestation techniques can provide a way to assess existing and past software configuration status so that deviations from expected norms can generate a notification or alarm event. Fifth, there must be a suitable means to detect a penetration of a meter(s) in a peer-to-peer mesh environment and isolate and contain any subsequent attempts to penetrate other devices. This is important, as one must assume that if an attacker has the capability to reverse engineer a device that any inbuilt protections can eventually be compromised. It is an open and challenging problem to do intrusion detection in a peer-to-peer mesh environment.

D.3.19 Side Channel Attacks on Smart Grid Field Equipment

A side-channel attack is based on information gained from the physical implementation of a cryptosystem, and is generally aimed at extracting cryptographic keys. For example, early smart card implementations were particularly vulnerable to power analysis attacks that could determine the key used by a smart card to perform a cryptographic operation by analysis of the card's power consumption. Tempest attacks similarly can extract data by analysis of various types of electromagnetic radiation emitted by a CPU, display, keyboard, etc. Van Eck phreaking in particular can reconstruct the contents of a screen from the radiation emitted by the CRT or LCD, and can be performed at some distance. Tempest attacks are nearly impossible to detect. Syringe attacks use a syringe needle as a probe to tap extremely fine wire traces on printed circuit boards. Timing attacks exploit the fact that cryptographic primitives can take different lengths of time to execute for different inputs, including keys. For all side channel attacks, it is not necessary for an attacker to determine the entire key, but only enough of the key to facilitate use of other code breaking methods.

Smart grid devices that are deployed in the field, such as substation equipment, pole-top equipment, smart meters and collectors, and in-home devices, are at risk of side channel attacks due to their accessibility. Extraction of encryption keys by side channel attacks from smart grid equipment could lead to compromise of usage information, personal information, passwords, etc. Extraction of authentication keys by side channel attacks could allow an attacker to impersonate smart grid devices and/or personnel, and potentially gain administrative access to smart grid systems.

D.3.20 Securing and Validating Field Device Settings

Numerous field devices contain settings. A prominent example is relay settings that control the conditions such as those under which the relay will trip a breaker. In microprocessor devices,

these settings can be changed remotely. One potential form of attack is to tamper with relay settings and then attack in some other way. The tampered relay settings would then exacerbate the consequences of the second attack.

A draft NERC white paper on identifying cyber-critical assets recognizes the need for protecting the system by which device settings are determined and loaded to the field devices themselves. This can include the configuration management process by which the settings are determined. It should likely extend to ongoing surveillance of the settings to ensure that they remain the same as intended in the configuration management process.

D.3.21 Absolute & Accurate Time Information

Absolute time is used by many types of power system devices for different functions. In some cases, time may be only informational, but increasingly more and more advanced applications will critically depend on an accurate absolute time reference. According to the draft NERC CSSWG Guideline on Timestamping of Operational Data Logs, "these applications include, but are not limited to, Power Plant Automation Systems, Substation Automation Systems, Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IED), sequence of event recorders, digital fault recorders, intelligent protective relay devices, Energy Management Systems (EMS), Supervisory Control and Data Acquisition (SCADA) Systems, Plant Control Systems, routers, firewalls, Intrusion Detection Systems (IDS), remote access systems, physical security access control systems, telephone and voice recording systems, video surveillance systems, and log collection and analysis systems." Some detailed examples follow.

Security Protocols

Time has impact on multiple security protocols especially in regards to the integrity of authentication schemes and other operations if it is invalid or tampered with. For example some protocols can have reliance on time stamp information to ensure against replay attacks, or in other cases of time based revoked access. Due care needs to be taken to ensure time cannot be tampered with in any system as well as ensuring if it is that it can be detected, responded to, and contained.

Synchrophasors

Syncrophasor measurement units are increasing being deployed throughout the grid. A phasor is a vector consisting of magnitude and angle. The angle is a relative quantity, and can be interpreted only with respect to a time reference. A synchrophasor is a phasor that is calculated from data samples using a standard time signal as the reference for the sampling process. Initial deployments of synchrophasor measurement units use synchrophasors to measure the current state of the power system more accurately than it can be determined through state estimation. If the time references for enough synchrophasor measurements are incorrect, the measured system state will be incorrect, and corrective actions based on this inaccurate information could lead to grid destabilization.

Synchrophasor measurements are beginning to be used to implement wide area protection schemes. With inaccurate time references, these protection schemes may take inappropriate corrective actions that may further destabilize the system.

Certificates

Certificates are typically used to bind an identity to a public key or keys, facilitating such operations as digital signatures and data encryption. They are widely used on the internet, but there are some potential problems associated with their use.

Absolute time matters for interpretation of validity periods in certificates. If the system time of a device interpreting a certificate is incorrect, an expired certificate could be treated as valid or a valid certificate rejected as expired. This could result in incorrect authentication or rejection of users, incorrect establishment or rejection of VPN tunnels, etc. Kerberos (on which Windows domain authentication is based) also depends critically on synchronized clocks.

Event Logs and Forensics

Timestamps in event logs must be based on accurate time sources so that logs from different systems and locations can be correlated to reconstruct historical sequences of events. This applies both to logs of power data and to logs of cyber security events. Correlating power data from different locations can lead to understanding of disturbances and anomalies, and difficulties in correlating logs was a major issue in investigating the August 14, 2003 blackout. Correlating cyber security events from different systems is essential to forensic analysis to determine if and how a security breach occurred and to support prosecution.

D.3.22 Personnel Issues In Field Service Of Security Technology

Device security features or security devices themselves may add to labor complexity if field personnel have to interact with these devices in any way to accomplish maintenance and installation operations. This complexity may mean significant increases in costs that can lead to barriers for security features and devices being used. Thus due care must be taken when introducing any security procedures and technology to ensure their management requires minimum disruption to affected labor resources.

For instance, some utilities operate in regulated labor environments. Contractual labor agreements can impact labor costs if field personnel have to take on new or different tasks to access, service, or manage security technology. This can mean a new class or grade of pay and considerable training costs for a large part of the organization. In addition there are further complexities introduced by personnel screening, clearance, and training requirements for accessing cyber assets.

Another potential ramification of increased labor complexity due to security provisions can occur if employees or subcontractors have financial incentive to bypass or circumvent the security provisions. For example, if a subcontractor is paid by the number of devices serviced, anything that slows down production, including both safety and security measures, directly affects the bottom line of that subcontractor, giving rise to an unintended financial motivation to bypass security or safety measures.

D.3.23 Weak Authentication of Devices In Substations

Inside some substations, where the components are typically assumed to be in a single building or enclosure, access control protection may be weak, as physical security is assumed to exist. For example, some systems may provide access control by MAC address filtering. When a

substation is extended to incorporate external components such as solar panels, wind turbines, capacitor banks, etc. that are not located within the physical security perimeter of the substation, this protection mechanism is no longer sufficient.

An attacker who gains physical access to an external component can then eavesdrop on the communication bus, and obtain (or guess) MAC addresses of components inside the substation. Indeed, the MAC addresses for many components are often physically printed or stamped on the component. Once obtained, the attacker can fabricate packets that have the same MAC addresses as other devices on the network. The attacker may therefore impersonate other devices, re-route traffic from the proper destination to the attacker, and perform man-in-the-middle attacks on protocols that are normally limited to the inside of the substation.

D.3.24 Weak Security for Radio-Controlled Distribution Devices

Remotely controlled switching devices that are deployed on pole-tops throughout distribution areas have the potential to allow for faster isolation of faults and restoration of service to unaffected areas. Some of these products that are now available on the market transmit open and close commands to switches over radio with limited protection of the integrity of these control commands. In some cases no cryptographic protection is used, while in others the protection is weak in that the same symmetric key is shared amongst all devices.

D.3.25 Weak Protocol Stack Implementations

Many IP stack implementations in control systems devices are not as evolved as the protocol stacks in modern general-purpose operating systems. Improperly formed or unexpected packets can cause some of these control systems devices to lock up or fault in unexpected ways.

D.3.26 Insecure Protocols

Few if any of the control systems communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures. This applies to both serial protocols and IP protocols, such as DNP over TCP. IEC 62351 (which are the security standards for these protocols) is now available but implementation adoption and feasibility is not yet clear. There is a secure authentication form of DNP3 under development.

D.4 Non-Specific Cyber Security Issues

This section lists cyber security issues that are too abstract to describe specific security problems, but when considered in different contexts (control center, substation, meter, HAN device, etc.) are likely to lead to specific problems.

D.4.1 IT vs. Smart Grid Security

The differences between IT, industrial, and Smart Grid security needed to be accentuated in any standard, guide, or roadmap document. NIST SP800-82 can be used as a basis but more needs to be addressed as control system security operates in an industrial campus environment and is not the same as something that has the scale, complexity, and distributed nature of the Smart Grid.

D.4.2 Patch Management

Specific devices such as IEDs, PLCs, Smart Meters, etc. will be deployed in a variety of environments and critical systems. Their accessibility for software upgrades or patches maybe a complex activity to undertake because of how distributed and isolated equipment can be. Also there are many unforeseen consequences that can arise from changing firmware in a device that is part of a larger engineered system. Control systems require considerable testing and qualification to maintain reliability factors.

The patch, test and deploy lifecycle is fundamentally different in the electrical sector. It can take a year or more (for good reason) to go through a qualification of a patch or upgrade. Thus there are unique challenges to be addressed in how security upgrades to firmware needs to be managed.

Deployment of a security upgrade or patch is unlikely to be as rapid as in the IT industry. Thus there needs to be a process where by the risk and impact of vulnerability can be determined in order to prioritize upgrades. Also a security infrastructure needs to be in place that can mitigate possible threats until the upgrade can be qualified and deployed so that the reliability of the system can be maintained.

D.4.3 Authentication

There is no centralized authentication in the de-centralized nature of the grid. Authentication systems need to be able to operate in the massively distributed and locally autonomous environment. For example, substation equipment such as IEDs needs to have access controls that only allow for authorized users to configure or operate them. However, the credential management of such systems cannot assume that a constant network connection exists to a central office to be used in their authentication processes. There needs to be secure authentication methods that allows for local autonomy when needed and yet can provide for the revocation and attribution from a central authority as required. Equally important is any authentication processes must securely support emergency operations and not become an impediment at a critical time.

D.4.4 System Trust Model

There has to be a clear idea of elements of the system are trusted and to what level and why. Practically speaking there will always be something you have to trust in the system. We must identify the technologies, people, and processes that form the basis of that trust. For example we could trust a private network infrastructure more than an open public network because it has a basis of less risk. However, even this statement has its own dependencies based on the design and management of that network that would inform the trust that is being vested in it.

D.4.5 User Trust Model

Today and in the future, many operational areas within the Smart Grid are managed and maintained by small groups of trusted individuals operating as close-knit teams. These individuals are characterized by multi-decade experience and history in their companies. Examples include distribution operations departments, field operations and distribution engineering/planning. Security architectures designed for large scale, public access systems such

as credit card processing, database applications, etc. may be completely inappropriate in such settings and actually weaken security controls. IT groups will almost always be required for proper installation of software and security systems on user PCs. However, for these unique systems, administration of security assets, keys, passwords etc. that require heavy ongoing dependence on IT resources may create much larger and unacceptable vulnerabilities.
In terms of personnel security, it may be worthwhile considering what is known as "two-person integrity", or TPI for short. TPI is a security measure to prevent single person access to key management mechanisms. This comes from national security environments, but may have some applicability to the smart grid. This is somewhat similar to safety and having at least two people working in hazardous environments.

Another area of concern related to personnel issues has to do with not having a backup to someone having a critical function - in other words, a person (actor) as a single point of failure (SPOF).

D.4.6 Security Levels

A security model needs to be built with different security levels that depend on the design of the network/system architecture, security infrastructure, and how trusted the overall system and its elements are. This model can help put the choice of technologies and architectures within a security context and guide the choice of security solutions.

D.4.7 Distributed vs. Centralized Model of Management

There are unique issues of how to manage something as distributed as the Smart Grid and yet maintain good efficiency and reliability factors that imply centralization. Many systems are highly distributed, geographically isolated, and require local autonomy, as commonly found in modern substations. Yet these systems need to have a measure of centralized security management in terms of event logging/analysis, authentication, etc. There needs to be a series of standards in this area that can strike the right balance and provide for a hybrid approach that is necessary for the Smart Grid.

D.4.8 Local Autonomy of Operation

Any security system must have local autonomy, as for example one cannot always assume a working network link back to a centralized authority, and particularly in emergency oriented operations it cannot be the security system that denies critical actions to be taken.

D.4.9 Intrusion Detection for Power Equipment

One issue specific to power systems is handling specialized protocols like Modbus, DNP3, 61850, etc. Their needs to be standardized IDS and security event detection and management models built for these protocols and systems. More specifically these models need to have a deep contextual understanding of device operation and state to be able to detect when anomalous commands might create an unforeseen and undesirable impact.

D.4.10 Network and System Monitoring and Management for Power Equipment

Power equipment does not necessarily use common and open monitoring protocols and management systems. They are often a fusion of proprietary or legacy based protocols with their

own security issues. There is a need for openly accessibility information models and protocols that can be used over a large variety of transports and devices. There might even be a need for bridging power equipment into traditional IT monitoring systems for their cyber aspects. The management interfaces themselves must also be secure, as early lessons with SNMP have taught the networking community. Also and very importantly the system monitoring and management will have to work within a context of massive scale, distribution, and often bandwidth limited connections.

D.4.11 Security Event Management

Building on more advanced forms of IDS for Smart Grid, security monitoring data/information from a wide array of power and network devices/systems must start to become centralized and analyzed for detecting events on a correlated basis. There also needs to be clear methods of incident response to events that is coordinated between control system and IT groups. Both of these groups must be involved in security event definition and understanding as only they have the necessary operational understanding for their respective domains of expertise to understand what subtleties could constitute a threat.

D.4.12 Cross-Utility/Cross-Corporate Security

Unfortunately many smart grid deployments are going forward with not much thought to what happens behind the head end systems for AMI as well as further on down the line for SCADA and other real-time control systems backing up substation automation and other distribution automation projects as well as the much larger transmission automation functions. Many utilities have not thought about how call centers and demand response control centers will handle integration with head end systems. Moreover, in many markets, the company that controls the head end to meter portion is different than the one who decides what load to shed for a demand response. In many cases those interconnections and the processes that go along with them have yet to be built or even discussed. Even in a completely vertically integrated, there are many challenges with respect to separation of duties and least privilege versus being able to get the job done when needed. This also means designing application interfaces that are usable for the appropriate user population and implement threshold controls, so someone can't disconnect hundreds of homes in a matter of a few seconds accidentally or maliciously.

D.4.13 Trust Management

Appropriate trust of a device must be based on the physical and logical ability to protect it (and of course, the design of the network).

For instance, trusting a meter for usage readings is a necessary risk, and the impact of incorrect readings is minimal (short of buffer and integer overruns). However, because physical protections on a meter are nearly nonexistent, they should not be allowed to communicate directly with highly critical systems, as in existing WiMAX deployments, where the meter communicates directly with the head end, which may control a significant amount of load. An attack on the meter may result in compromise of the head end.

Similarly, because most pole-top devices have very little physical protection, the level of trust for those devices must be limited accordingly. An attacker could replace the firmware, or, in many systems, simply place a malicious device between the pole-top device and the network

connection to the Utility network, since these are often designed as separate components with RJ45 connectors. If the head end system for the pole-top devices places too much trust in them, a successful attack on a pole-top device can be used as a stepping stone to attack the head end. Trust Management lays out several levels of trust, based on physical and logical access-control and criticality of the system (i.e. we make most decisions based on how important this system is). In this type of Trust Management, we categorize each system in the Smart Grid, not only for its own needs (AIC, etc...) but by our required and/or limitations of trust mandated by our ability to control physical and logical access to it and desire to do so (criticality of the system). This will lead to a more robust system, where compromise of a less trusted component will not easily lead to compromise of more trusted components.

D.4.14 Management of Decentralized Security Controls

Many security controls such as authentication and monitoring may operate in autonomous and disconnected fashion because of the often remote nature of grid elements (e.g. remote substations). However, for auditing and centralized security management (e.g. revocation of credentials) requirements this presents unique challenges.

D.4.15 Password Management

Passwords for authentication and authorization (e.g., in lieu of stronger multi-factor authentication) have many problems when used with highly distributed, decentralized, and variedly connected systems such as the Smart Grid. Where possible, passwords alone should be avoided, but some use of passwords will be – and already is – inevitable. Suitable password management schemes need to be developed that take into account both the nature of smart grid systems and of users.

D.4.16 Cipher Suite

A cipher suite that is open (e.g. standards based, mature, and preferably patent free) and reasonably secure for wide application in Smart Grid systems would help enable interoperability. Factors to consider are which block ciphers (e.g. 3DES, AES) are appropriate in which modes (CBC, CTR, etc.), key sizes, and asymmetric ciphers (e.g. ECC, RSA, etc.) that could form the basis for many authentication operations. The FIPS standards and particularly FIPS-140-2 are a guide, as well as the NSA Suite B algorithms. Device profile, data temporality/criticality/value should also play a role in cipher and key strength selection.

D.4.17 Authenticating Users to Control Center Devices and Services

Control center equipment based on modern operating systems such as Unix or Windows platforms is amenable to standard Enterprise solutions such as RADIUS, LDAP, or Active Directory. Nevertheless, these mechanisms may require modification or extension in order to incorporate “break glass” access or to interoperate with access mechanisms for other equipment. Some access policies commonly used in enterprise systems, such as expiring passwords and locking screen savers, are not appropriate for operator consoles.

Federated identity/authentication management systems may be appropriate here due to the variety of different kinds of authentication systems that will need to be integrated.

D.4.18 Authentication of Devices to Users

When accessing smart grid devices locally, such as connecting to a meter via its optical port, authentication of the device to the user is generally not necessary due to the proximity of the user. When accessing smart grid devices via a private secure network such as a LAN in a substation tunneled to the control center, or an AMI network with appropriate encryption, non-secure identification of devices, such as by IP address, may be sufficient.
A similar problem to this is that of ensuring that the correct web server is reached via a website address. In web systems this problem is solved by SSL certificates that include the DNS name of the server.

D.4.19 Entropy

Many devices do not have access to sufficient sources of entropy to serve as good sources of randomness for cryptographic key generation and other cryptographic operations. This is a fundamental issue and has impacts on the key management and provisioning system that must be designed and operated in this case.

D.4.20 Tamper Evidence

In lieu of or in addition to tamper resistance, tamper evidence will be desirable for many devices. Both tamper resistance and tamper evidence must be resistant to false positives in the form of both natural actions, such as earthquakes, and adversarial actions. Tamper evidence for meters cannot require physical inspection of the meter since this would conflict with zero-touch after installation, but physical indicators might be appropriate for devices in substations.

D.4.21 Challenges with Securing Serial Communications

Cryptographic protocols such as TLS can impose too much overhead on bandwidth-constrained serial communications channels. Bandwidth conserving and latency sensitive methods are required in order to secure many of the legacy devices that will continue to form the basis of many systems used in the Grid.

D.4.22 Legacy Equipment with Limited Resources

The lifecycle of equipment in the electricity sector typically extends beyond 20 years. Compared to IT systems, which typically see 3-5 year lifecycles, this is an eternity. Technology advances at a far more rapid rate, and security technologies typically match the trend. Legacy equipment, being 20 years old or more, is resource limited and it is difficult and in some cases impractical to add security to the legacy device itself without consuming all available resources or significantly impacting performance to the point that the primary function and reliability of the device is hindered. In many cases, the legacy device simply does not have the resources available to upgrade security on the device through firmware changes. Security needs to be developed in such a manner that it has a low footprint on devices so that it can scale beyond 20 years and more needs to be done to provide a systemic and layered security solution to secure the system from an architectural standpoint.

D.4.23 Costs of Patch and Applying Firmware Updates

The costs associated with applying patches and firmware updates to devices in the electricity sector are significant. The balance of the cost versus the benefit of the security measure in the

risk mitigation and decision process can sometimes be prohibitive for the deployment if the cost outweighs the benefits of the deployment of the patch. Decision makers may choose to accept the risk if the cost is too high compared to the impact.

The length of time to qualify a patch or firmware update, and lack of centralized and remote patch/firmware management solutions contribute to higher costs associated with patch management and firmware updates in the electricity sector. Upgrades to devices in the electricity sector can take a year or more to qualify. The extensive regression testing is extremely important to ensure that an upgrade to a device won't negatively impact reliability, but also adds cost. Once a patch or firmware update is qualified for deployment, asset owners typically need to perform the upgrade at the physical location of the device due to a lack of tools for centralized and remote patch/firmware management.

D.4.24 Forensics and Related Investigations

It is already well-known that industrial control systems do not generate a lot of security event data and typically do not report it back to a centralized source on a regular basis. Depending on the device, system health, usage, and other data may get relayed back to data historians and/or maintenance management systems. Furthermore, as a matter of business policy, when faced with potential cyber security threats, electric utilities prioritize their obligation to maintain electric service over the requirements of evidence collection needed to properly prosecute the perpetrators. With smart grid technology, additional threats are arising that may require a greater capability for generating and capturing data. Technologically sophisticated devices such as smart meters are being publicly exposed. At minimum, the meters should be capable of detecting and reporting physical tampering to identify energy theft or billing fraud. Moreover, HAN level equipment will need to interact with the meter to support demand response. That means having the tools and data to diagnose any problems resulting from either intentional manipulation or other causes. While it is rare that computer forensics is ever the sole basis for a successful prosecution or civil suit, it is critical that reliable means be defined and the tools provided to maintain chain of custody, reduce the risk of spoliation, and ensure that its origin can be properly authenticated. Tools should be capable of retrieving data from meters, collectors, head end systems as well as other embedded systems in substations, commercial and industrial customer equipment, and sensors along the lines in a read-only manner either at the source or over the network.

D.4.25 Roles and Role Based Access Control

A role is a collection of permissions that may be granted to a user. A given user may be given several roles, or may be permitted different roles in different circumstances, and may thereby exercise different sets of permissions in different circumstances.
Roles clearly need to relate to the structure of the using entity and its policies regarding appropriate access. Both the structure and access policies properly flow down from regulatory requirements and organizational governance (i.e., from the high, non-technical levels of the GWAC stack).

Issues in implementing RBAC include the following:

1. The extent to which roles and roles should be pre-defined in standards versus providing the flexibility for individual entities to define their own. Is there a suitable default set of roles that is applicable to the majority of the utility industry, but can be tailored to the needs of a specific entity? Such roles might include:
   - Auditors: users with the ability to only read/verify the state of the devices (this may include remote attestation).
   - System dispatchers: Users who perform system operational functions in control centers.
   - Protection engineers: Users who determine and install/update settings of protective relays and retrieve log information for analysis of disturbances.
   - Substation maintainers: Users who maintain substation equipment and have access requirements to related control equipment.
   - Administrators: users who can add, remove or modify the rights of other users;
   - Security officers: users who are able to change the security parameters of the device (e.g. authorize firmware updates).
2. Management and usability of roles. How many distinct roles become administratively unwieldy?
3. Policies need to be expressed in a manner that is implementable and relates to an entity's implemented roles. Regulators and entity governance need guidance on how to express implementable policies.
4. Support for non-hierarchical roles. The best example is originator and checker (e.g., of device settings). Any of a group of people can originate and check, but the same person can't do both for the same item.
5. Approaches to expressing roles in a usable manner.
6. Support for emergency access that may need to bypass normal role assignment.
7. Which devices need to support RBAC? Which do not?

D.4.26 Limited Sharing of Vulnerability and/or Incident Information

There is a significant reticence to sharing information about vulnerabilities or incidents in any critical infrastructure industry. This is based on many sound reasons. The least of which is the fact that lives could be on the line and that it can take a considerable amount of time to qualify an upgrade or patch to fix any issue in complex control systems. There needs to exist a better framework for securely sharing such information and quickly coming to field level mitigations until infrastructure can be upgraded. There also needs to be a better system of accountability and confidentiality when sharing sensitive vulnerability information with any 3rd party be it government or private institution.

D.4.27 Data Flow Control Vulnerability Issue

The grid will encompass many networks and sub-networks and the challenge will be to regulate which system can access or talk to another system.

If a user on system A is authorized to perform device firmware upgrade on device A, if device A is moved (stolen, replaced etc) to system B, how is the authorization tracked? How do you ensure that the control information is not being diverted to another unauthorized device/system? There is probably a need for intersection of security at various layers.

D.4.28 Public vs. Private Network Use

There is on-going debate in the industry over the use of public network infrastructure such as the Internet or public cellular or WiMax networks that telecommunication companies provide. A public network is not be confused with the use of the Internet Protocol (IP) in a private network infrastructure. The reality is that many elements of the Smart Grid might already or will in future make use of public networks. The cyber security risks that this introduces need to be addressed by a risk management framework and model that takes this reality into account. It should be clear that if critical real-time command and control functions are carried over public networks, such as the Internet (even if technically possible), this carries significantly more risk of intrusion, disruption, tampering, and general reliability regardless of countermeasure. This is by the sheer accessibility of the system by anyone in the world regardless of location and the fact that countermeasures are routinely defeated because of errors in configuration, implementation and sometimes design. These facts should be self evident in a risk metric that a model would produce.

Any risk management framework would be well served to address this issue by:

- Building a model that takes the nature of the network, its physical environment, and its architecture into account (e.g. is it private or public, is critical infrastructure sufficiently segmented away from general IT networks, is there physical protection/boundaries, etc.)
- Assigning criticality and impact levels to smart grid functions/applications (e.g. retrieval of metering data is not as critical as control commands)
- Identifying countermeasure systems (e.g. firewalls, IDS/IPS, SEM, Encrypted links & data, etc.) and assigning mitigating levels as well as which smart grid functions they can reasonably be applied to and how.

The end goal for the model should be to make the best security practices self-evident through a final quantitative metric without giving a specific prohibition.

D.4.29 Traffic Analysis

Traffic Analysis is the examination of patterns and other communications characteristics to glean information. Such examination is possible, even if the communication is encrypted. Examples of relevant characteristics include:

- The identity of the parties to the communication (possibly determined from address or header information sent “in the clear” even for otherwise encrypted messages)
- Message length, frequency, and other patterns in the communications
- Characteristics of the signals that may facilitate identification of specific devices, such as modems. An example of such a characteristic might be the detailed timing or shape of the waveforms that represent bits.

Regulations such as FERC 889 establish "Standards of Conduct" that prohibit market participants from having certain information on the operational state of the grid as known to grid control centers. In the Smart Grid, future regulations could possibly extend this concept to information outside the bulk power domain. Traffic analysis could enable an eavesdropper to gain information prohibited by such regulations. In addition, even if operational information were encrypted, traffic analysis could provide an attacker with enough information on the operational situation to enable more sophisticated timing of physical or cyber attacks.

D.4.30 Poor Software Engineering Practices

Poor software engineering practices, such as those identified in the Vulnerabilities Section of NISTIR 7628, can lead to software that misoperates and may represent a security problem. Such problems are well known in software, but it should be recognized that embedded firmware may also be susceptible to such vulnerabilities [IOActive], and that many of the same good software engineering practices that help prevent these vulnerabilities in software may also be used for that purpose with firmware.

D.4.31 Attribution of Faults to the Security System

When communications or services fail in networks, there is sometimes a tendency to assume this failure is caused by the security system. This can lead to disabling the security system temporarily, during problem resolution, or even permanently if re-enabling security is forgotten. Security systems for the smart grid need to allow and support troubleshooting.

D.4.32 Need for Unified Requirements Model

Within each operating domain (such as distribution operations, control center operations, etc.) multiple, ambiguous or potentially conflicting implementation requirements must be resolved and settled-on. If security advisors cannot know what to expect from products meeting a certain standard then each acquisition cycle will involve a unique security specification. Under such circumstances it will be nearly impossible for suppliers to provide products in a timely fashion and diverse systems will be difficult or impossible for customers to administer. The scope of this effort should cover such things as password complexity, required security roles, minimum numbers of supported user IDs, etc.

D.4.33 Utility Purchasing Practices

Unlike many other industries, many customers (Utilities) in the Utility Industry are large-enough, and have enough purchasing power and longevity (these companies have very long histories and steady income) to be able to specify unique, often customer-specific product features and requirements. For example, prior to the advent of the DNP3 communication protocol, in North America alone there were over 100 different SCADA protocols developed over the period from roughly 1955 to 1990. Many of these protocols were unique due to a customer requirement for what may have appeared to be a minor change, but one which made their protocol implementation unique.

Recently there have been efforts by region, state, and regulatory entities to create purchasing requirements. If not carefully coordinated, these efforts could have similar harmful effects.

With regard to cyber security requirements, if security requirements are subject to interpretation, customers will each use their own preferences to specify features that will re-create the problem of the SCADA protocols. For the smart grid, this would be a serious problem, since the time and effort necessary to analyze, negotiate, implement, test, release and maintain a collection if customer-specific implementations will greatly delay deployment of the smart grid. Specifically, with regard to the smart grid, recent procurements have shown little consistency, each calling out different requirements. This can have an adverse affect on both interoperability and security.

D.4.34 Cyber Security Governance

From the IT Governance Institute, and adopted by the Chartered Institute of Management Accountants (CIM and the International Federation of Accountants (IFAC), governance is defined as the following:
"Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."

Cyber security governance is really a subset of enterprise governance. What's included in enterprise governance that directly impacts cyber security governance is strategic direction of the smart grid, ensuring that goals and objectives are achieved, business risk (includes security risk) is managed appropriately, resource utilization is efficiently and effectively managed in a responsible fashion, and enterprise security activities are monitored to ensure success or risk mitigation is needed if there are failures in security.
Since cyber security (information security), as opposed to IT security, has an overall perspective on all aspects of data/information, meaning spoken, written, printed, electronic, etc., and how it's handled through creation, how the data/information is viewed, how it's transported, stored and/or destroyed, it is up to the utility's board and executive management to ensure that the smart grid, as well as the overall electric grid, is protected as much as feasibly possible.
The utility's Board of Directors and Executive Management must be cognizant of the risks that must be taken into account regarding what vulnerabilities to security threats of any sort if smart grid systems are not created and managed carefully, and how such risks may be mitigated (SEC. 1309, EISA 2007).

Borrowing from the IT Governance Institute's guide to "Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition", following is a slightly edited perspective on the responsibilities of a utility's Board of Directors and Executive Management team regarding cyber security.

Utility's Boards of Directors/Trustees

It is a fundamental responsibility of Senior Management to protect the interests of the utility's stakeholders. This includes understanding risks to the business and the electric grid to ensure they are adequately addressed from a governance perspective. Doing so effectively requires risk management, including cyber security risks, by integrating cyber security governance into the overall enterprise governance framework of the utility.

Cyber security governance for the electric grid as a whole requires strategic direction and impetus. It requires commitment, resources and assignment of responsibility for cyber and information security management, as well as a means for the Board to determine that its intent has been met for the electric grid as part of the critical infrastructure of the United States. Experience has shown that effectiveness of cyber security governance is dependent on the involvement of senior management in approving policy, and appropriate monitoring and metrics coupled with reporting and trend analysis regarding threats and vulnerabilities to the electric grid.

Members of the Board need to be aware of the utility's information assets and their criticality to ongoing business operations of the electric grid. This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analysis. It may also be accomplished by business dependency assessments of information resources. A result of these activities should include Board Members validating/ratifying the key assets they want protected and confirming that protection levels and priorities are appropriate to a recognized standard of due care.

The tone at the top (top-down management) must be conducive to effective security governance. It is unreasonable to expect lower-level personnel to abide by security policies if senior management does not. Visible and periodic board member endorsement of intrinsic security policies provides the basis for ensuring that security expectations are met at all levels of the enterprise and electric grid. Penalties for non-compliance must be defined, communicated and enforced from the board level down.

Utility Executives

Implementing effective cyber security governance and defining the strategic security objectives of the utility are complex, arduous tasks. They require leadership and ongoing support from executive management to succeed. Developing an effective cyber security strategy requires integration with and cooperation of business unit managers and process owners. A successful outcome is the alignment of cyber security activities in support of the utility's objectives. The extent to which this is achieved will determine the effectiveness of the cyber security program in meeting the desired objective of providing a predictable, defined level of management assurance for business processes and an acceptable level of impact from adverse events.
An example of this is the foundation for the U.S. federal government's cyber security, which requires assigning clear and unambiguous authority and responsibility for security, holding officials accountable for fulfilling those responsibilities, and integrating security requirements into budget and capital planning processes.

Utility Steering Committee

Cyber security affects all aspects of the utility. To ensure that all Stakeholders affected by security considerations are involved, a Steering Committee of Executives should be formed. Members of such a committee may include, amongst others, the Chief Executive Officer (CEO) or designee, business unit executives, Chief Financial Officer (CFO), Chief Information Officer (CIO)/IT Director, Chief Security Officer (CSO), Chief Information Security Officer (CISO), Human Resources, Legal, Risk Management, Audit, Operations and Public Relations.

A Steering Committee serves as an effective communication channel for Management's aims and directions and provides an ongoing basis for ensuring alignment of the security program with the utility's organizational objectives It is also instrumental in achieving behavior change toward a culture that promotes good security practices and policy compliance.

Chief Information Security Officer

All utility organizations have a CISO whether or not anyone actually holds that title. It may be the CIO, CSO, CFO or, in some cases, the CEO, even when there is an Information Security Office or Director in place. The scope and breadth of cyber security concerns are such that the authority required and the responsibility taken inevitably end up with a C-level officer or Executive Manager. Legal responsibility, by default, extends up the command structure and ultimately resides with Senior Management and the Board of Directors.

Failure to recognize this and implement appropriate governance structures can result in Senior Management being unaware of this responsibility and the attendant liability. It usually results in a lack of effective alignment of security activities with organizational objectives of the utility. Increasingly, prudent and proactive management is elevating the position of Information Security Officer to a C-level or Executive Position as utilities begin to understand their dependence on information and the growing threats to it. Ensuring that the position exists, and assigning it the responsibility, authority and required resources, demonstrates Management's and Board of Directors' awareness of and commitment to sound cyber security governance.

D.5 Design Considerations

This section discusses cyber security design considerations that arise in the design, deployment, and use of smart grid systems, and should be taken into account by system designers, implementers, purchasers, integrators, and users of smart grid technologies. In discussing the relative merits of different technologies or solutions to problems, these design considerations stop short of recommending specific solutions or even requirements.

D.5.1 Cryptography, Key Management, and PKI

Secure key management is essential to the effective use of cryptography in deploying a Smart Grid infrastructure. NIST SP 800-57 Part 1 recommends best practices for developers and administrators on secure key management. These recommendations are as applicable for the Smart Grid as for any other infrastructure that make use of cryptography, and are a starting point for Smart Grid key management. Please see the R&D topics section on a discussion of some of the considerations.

Computational Constraints

Some smart grid devices, particularly residential meters and in-home devices, may be constrained in computational power. These constraints may make public key cryptography or even any cryptography at all infeasible. Note, however, that the recent generations of most vendor's smart meters support symmetric encryption, and at least one supports public key cryptography (ECC).

Channel Bandwidth

The Smart Grid will involve communication over a variety of channels with varying bandwidths. Encryption alone does not generally impact channel bandwidth, since symmetric ciphers such as AES produce roughly the same number of output bits as input bits, except for rounding up to the cipher block size. However, encryption negatively influences lower layer compression algorithms since encrypted data is uniformly random and therefore not compressible. For compression to be effective, compression must be performed before encryption, and this must be taken into account in designing the network stack.

Integrity protection as provided by a Message Authentication Code (MAC) adds a fixed overhead to every message, typically 256 bits or more. On slow channels that communicate primarily short messages, this overhead can be significant. For instance, SEL's Mirror Bits protocol for line protection continuously exchanges 8-bit messages. Protecting these messages with a 256 bit MAC would markedly impact latency unless the channel bandwidth was significantly increased.

Low bandwidth channels may be too slow to exchange large certificates frequently. If the initial certificate exchange is not time critical and is used to establish a shared symmetric key(s) that is used for an extended period of time, as with IKE, certificate exchange can be practical over even slow channels. However, if the certificate-based key-establishment exchange is time critical, protocols such as IKE that exchange multiple messages before arriving at a pre-shared key may be too expensive, even if the size of the certificate is minimal.

Distribution of certificates on the internet is typically done via public key infrastructure (PKI), and relies on chains of certificates to validate individual end certificates. Adapting such an infrastructure to computationally and bandwidth constrained devices is a non-trivial problem, and certificates are often 2K in size. A typical web browser (e.g. Firefox 3.0.14) ships with 140 built-in certificates. Because this may represent 100K or more, it also may present a storage challenge for some classes of non-computer devices.

Connectivity

Standard PKI systems based on a peer-to-peer key establishment model where any peer may need to communicate with any other may not be necessary or desirable from a security standpoint for components in the smart grid. Many devices may not have connectivity to key servers, certificate authorities, OCSP servers, etc.

Many connections between smart grid devices will have much longer durations (often permanent) than typical connections on the Internet.

Certificate Lifecycles

Background

Certificates are issued with a validity period. The validity period is defined in the X509 certificate with two fields called “notBefore” and “notAfter”. The notAfter field is often referred to as the expiration date. As will be shown below, it is important to only consider certificates as valid if they are being used during the validity period.

If it is determined that a certificate has been issued to an entity that is no longer trustworthy (for example the cert was issued to a device that was lost or stolen or sent to a repair depot), the certificate can be revoked. Certificate revocation lists (CRLs) are used to store the certificate serial number and revocation date for all revoked certificates. An entity that acts in reliance on a certificate is called a relying party (RP). To determine if the RP can accept the certificate, the RP needs to check, at a minimum, the following;

1. The certificate was issued by a trusted CA (This may require the device to provide, or the RP to obtain, a chain of certificates back to the RP's trust anchor.)
2. The certificates being validated (including any necessary chain back to the RPs trust anchor) are being used between the notBefore and notAfter dates.
3. The certificates are not in an authoritative Certificate Revocation List (CRL).
4. Other steps may be required depending on the RP's local policy, such as verifying that the distinguished name of the certificate subject, or the certificate policy fields are appropriate for the given application for which the certificate is being used.

For the purposes of this section we will focus primarily on steps 2 and 3.

Proper use of CRL, and Expiration Dates of Certificates

As mentioned above, when a certificate subject (person or device) is no longer trustworthy or the private key has been compromised, the certificate is placed into a CRL. This allows RPs to check the CRL to determine a certificate's validity status, by obtaining a recent copy of the CRL and determining whether or not the certificate is listed. Over time, a CRL can become very large as more and more devices are replaced and no longer needed. To prevent the CRL from growing too large, PKI administrators determine an appropriate length of time for the validity period of the certificates being issued. When a previously revoked certificate has expired it does not need to be kept on the CRL any longer. This is because an RP will see that the certificate has expired and would not need to further check the CRL.

Administrators must consider the balance between issuing certificates with short validity periods and more operational overhead, but with more manageable sized CRLs, and issuing certificates with longer validity periods lower operational overhead, but with potentially unwieldy large CRLs.

When certificates are issued to employees whose employment status or level of responsibility may change every few years, it would be appropriate to issue certificates with relatively short lifetimes such as a year or two. In this way, if an employee's status changes, and it becomes necessary to revoke his/her certificate, then this certificate would only need to be maintained on the CRL until the certificates expiration date. In this way (by issuing relatively short lived certificates), the CRLs can be kept to a reasonable size.

When certificates are issued to devices that are expected to last for many years or even decades, and these devices are housed in a secure environment, it may not be necessary to issue certificate with such short validity periods, as the likelihood of ever needing to revoke a certificate is low. Therefore the CRLs would not be expected to be very large. The natural question arises, when a smart grid RP receives a certificate from an entity (person or device) and the certificate is

expired, should the RP accept the certificate and authenticate the entity, or should the RP reject the certificate? What if rejecting the certificate will cause a major system malfunction?
First let's consider that smart grid devices will be deployed with the intent to keep them operational for many years (probably in the neighborhood for 20 to 30 years). Therefore, we would not expect to be replacing these devices very often. Of course there will be unplanned defects that will cause devices to be replaced from time to time. These devices will need to go on the CRL when they are removed from service, unless their keys can be guaranteed to be security destroyed. Because we do not want CRLs to grow without limit, it would be prudent to issue device certificates with an appropriate lifetime. For devices expected to last 20 years with a low MTBF which are housed in secure facilities, a 10 year certificate may be appropriate. This means that a device installed in the system (with a certificate), which subsequently fails, may need to be on a CRL for up to ten years.

If a good device never gets a new certificate before its certificate expires, the device will not be able to communicate in the system. To avoid this, the device could be provisioned to "renew" its certificate quite some time before its current certificate expires. For example, the device may be provisioned to renew its certificate a year before its current certificate expires. If the renewal attempt failed for any reason, the device would have a whole year to retry and obtain a new certificate. It is therefore easy to see that probability of a critical device not being able to participate in the system because of an expired certificate can be made as low as desirable by provisioning the device to renew its certificate with sufficient "lead time".

It is worth mentioning that because of the size and scale of the smart grid, other techniques may be needed to keep CRLs from growing excessively. These would include partitioning of CRLs into a number of smaller CRLs by "scoping" CRLs based on specific parameters, such as the devices' location in the network, the type of device, or the year in which the certificate was issued. Methods supporting such partitioning are documented in RFC 5280. Clearly with a system as large as the smart grid, multiple methods of limiting the size of CRLS will be required, but only with the use of reasonable expiration dates can CRLs be kept from growing without limit.

These methods should not be confused with techniques such as Delta CRLs, which allows CRLs to be fragmented into multiple files; or the use of the Online Certificate Status Protocol (OCSP), which allows an RP or certificate subject to obtain the certificate status for a single certificate from a certificate status server. These methods are useful for facilitating efficient use of bandwidth, however they do nothing to keep the size of the CRLs reasonable.

High Availability and Interoperability Issues of Certificates and CRLs

Certificate based authentication offers enormous benefits regarding high availability and interoperability. With certificate based authentication, two entities that have never been configured to recognize or trust each other can "meet" and determine if the other is authorized to access local resources or participate in the network. Through a techniques called "cross signing" or "bridging" these two entities may even come from different organizations, such as neighboring utilities, or a utility and a public safety organization. However, if CRLs are stored in central repositories, and are not reachable by RPs from time to time, due to network outages, it would not be always possible for RPs to determine the certificate status of the certificates that it

is validating. This problem can be mitigated in a number of ways. CRLs can be cached and used by RPs for lengthy periods of time, depending on local policy. CRLs can be scoped to small geographically close entities, such as all devices in a substation and all entities that the substation may need to communication with. These CRLs can then be stored in the substation to enhance their accessibility to all devices in the substation. One other alternative, which has the potential of offering very high availability, is where each certificate subject, periodically obtains it own signed certificate status, and caries it with him/her. When authenticating with an RP, the certificate subject not only provides its certificate but also it's most recent certificate status. If no other status source is available to the RP, and if the provided status is recent enough, the RP may accept this status as valid. This technique, sometimes referred to as OCSP Stapling, is supported by the common TLS protocol and is defined in RFC 4366. OSCP Stapling offers a powerful high availability solution for determining a certificate's status.

Other Issues relating to Certificate Status

- SmartGrid components may have certificates issued by their manufacturer. These certificates would indicate the make model and serial number of the device. If so, SmartGrid operators (e.g. utilities) should additionally issue certificates containing specific parameters indicating how the device is being used in the system. For example, certificate parameters could indicate that the subject is owned by Utility X, it is installed in Substation Y, and is authorized to participate in Application Z. These operator issued certificates could be new identity certificates which also contain these new attributes (possibly in the form of Certificate Policy Extensions) or they may be separate attribute certificates. Both options should be considered. For certificates issued to humans, attribute certificates may offer a more flexible solution since humans roles change. For certificates issued to devices, identity certificates that include attributes may offer a lower cost solution.
- Standardized Trust Management mechanisms would include standardized cross signing procedures, standardized policy constraints for cross signed certs, requirements for local and regional bridge providers, as well as approved methods to issue temporary credentials to entities during incidents involving exceptional system outages. Ideally such methods (for issuing temporary credential) would not be needed, as all entities would have their proper credentials before such an incident occurred. However, it is not unusual, after a large scale incident such as a hurricane, earthquake or a terrorist attack, that resources would be sent across country from sources that were never anticipated. There seem to be two general categories of solutions for such incidents. One is to make sure that all possible parties trust each-other beforehand. This type of solution may require too much risk, and require far too much operational overhead and unprecedented (and probably unnecessary) levels of trust and cooperation. The other method is to have a means of quickly issuing temporary local credentials to resources that arrived from remote sources. This method might rely on the resource's existing credentials from a remote domain, to support the issuance of new local credentials, possibly in the form of an attribute certificate.
- Standardized certificate policies for the Smart Grid would aid interoperability. Similar standards have been successful in other industries, such as the Financial Services industry with the X9.55 and X9.57 standards, and the health care industry with the ASTM

standard E2212 - 02a "Standard Practice for Healthcare Certificate Policy". At one extreme, this standard set of policies would define all possible roles for certificate subjects, it would define all categories of devices, and it would define specific requirements on the PKI participants for each supported assurance level. Further, such standards could include accreditation criteria for Smart Grid PKI service providers.

- Additional thought needs to go into determining what exactly should be authenticated between Smart Grid components. One could argue that not only is the identity of a component important, but also its authorization status, and its tamper status. The authorization status can be determined by roles, policies, or other attributes included in a certificate. However to determine a device's tamper status, the device will need to incorporate methods such as high assurance boot, secure software management, and local tamper detection via FIPS 140 mechanisms. Further the device will need to perform remote device attestation techniques to prove to others that the device has not been tampered with.
- Some certificate subjects should have secure hardware for storing private keys and trust anchor certificates. Due to the advent of the Smart Card market, such secure chips have become very affordable.
- RPs should have access to a reasonable accurate trustworthy source of time, to determine if a certificate is being used within its validity period.
- Further consideration should go into determining appropriate certificate lifetimes.

CRL Alternatives

There are two alternatives to a full-blown CRL; they are CRL partitions and OCSP. A CRL partition is simply a subset of a CRL; implementations exist that have partition tables with the status of as few as 100 certificates listed in it. For example, if a device needs to validate certificate number 3456, it would send a partition request to the domain CA. and the CA would send back a partition that addresses certificates 3400-3499. The device can use it to validate if the partner (or any other certificate in that range) has been revoked. Seeing that infrastructures are typically fixed, it is probable that a device will only interact with 1-20 other devices over its entire lifetime. So requesting and storing one to twenty ~1KB partition files is feasible compared to requesting and storing an "infinitely-long" CRL.

The other alternative is OCSP (Online Certificate Status Protocol) which, as the name implies, is an online, real-time service. OCSP is that is space optimal as it only stores valid certificates; there is no issue of an infinitely-long CRL; the OCSP repository is only as long as the number of valid certificates in the domain. Also OCSP has the added benefit of a real-time, positive validation of a certificate. With OCSP, when a device needs to validate a potential partner, it simply sends a validation request to OCSP Responder and it simply sends back an "OK" or "BAD" This approach requires no storage on the fielded device, but it does require the communications link to be active.

Local Autonomy of Operation

It may be important to support cryptographic operations such as authentication and authorization when connectivity to other systems is impaired or unavailable. For example, during an outage,

utility technicians may need to authenticate to devices in substations to restore power, and must be able to do so even if connectivity to the control center is unavailable. Authentication and authorization services must be able to operate in a locally autonomous manner at the substation.

Availability

Availability for some (but not all) smart grid systems can be more important than security. Dropping or refusing to re-establish connections due to key or certificate expiration may interrupt critical communications.

If one endpoint of a secure communication is determined by a third party to have been compromised, it may be preferable to simply should be a way of informing the other endpoint. This is true whether the key management is PKI or symmetric key based. In a multi-vendor environment it may be most practical to use PKI-based mechanisms to remove compromised devices.

Trust Roots

A typical web browser ships with a large number of built-in certificates (e.g. Firefox 3.0.14 ships with 140). It may not be appropriate for all of the Certificate Authorities that issue these certificates to be trust roots for smart grid systems. On the other hand, with third party data services (like Google PowerMeter) and load management services, it may not be appropriate for the utility to be the sole root of trust.

Additionally, there is a question about who issues certificates and how the system can assure that the claimed identity actually matches the certificate. The common method for internet use is that there are top-level (root) certificates that are the basis of all trust. This trust may be extended to secondary certificate issuing organization, but there is a question about how a root organization becomes a root organization, how they verify the identity for those requiring certificates, and even what identity actually means for a device.

Algorithms and Key Lengths

NIST SP800-57 recommends certain algorithms and key lengths. Any key management system used in the Smart Grid should carefully consider these guidelines and provide security considerations when deviating.

Selection and Use of Cryptographic Techniques

Designing cryptographic algorithms and protocols that operate correctly and are free of undiscovered flaws is difficult at best. There is general agreement in the cryptography community that openly published and time-tested cryptographic algorithms and protocols are less likely to contain security flaws than secretly developed ones because their publication enables scrutiny by the entire community. Historically, proprietary and secret protocols have frequently been found to contain flaws when their designs become public. For this reason, FIPS-approved and NIST-recommended cryptographic techniques are preferred where possible. However, the unique requirements that some parts of the Smart Grid place on communication protocols and computational complexity can drive a genuine need for cryptographic techniques that are not listed among the FIPS-approved and NIST recommended techniques. Known examples are PE Mode as used in IEEE P1711 and EAX as used in ANSI C12.22.

The general concerns are that these additional techniques have received a level of scrutiny and analysis commensurate with the standards development process of FIPS and recommendation practices of NIST. At a minimum a technique outside of this family of techniques should be (1) defined in a publicly available forum (2) published to a community of cryptographers for review and comment for a reasonable duration, (3) should be in, or under development in, a standard by a recognized standard development organization (SDO). In addition a case should be made for its use along the lines of resource constraints, unique nature of an application, or new security capabilities not afforded by the FIPS-approved and NIST-recommended techniques.

Elliptic Curve Cryptography (ECC)

The NSA has initiated a cryptographic interoperability strategy for U.S. Government systems. Part of this strategy has been to select a set of NIST-approved cryptographic techniques, known as Suite B, and foster adoption of these techniques through inclusion into standards of widely used protocols, like the IETF's TLS, S/MIME, IPSec, SSH. Suite B consists of the following NIST-approved techniques:

Encryption:
Advanced Encryption Standard (AES) - FIPS PUB 197 (with keys sizes of 128 and 256 bits)
See FIPS PUB 197 at the National Institute of Standards and Technology, FIPS Publications listing.

Key Exchange:
The Ephemeral Unified Model and the One-Pass Diffie Hellman (referred to as ECDH) - NIST Special Publication 800-56A (using the curves with 256 and 384- bit prime moduli)

Digital Signature:
Elliptic Curve Digital Signature Algorithm (ECDSA) – FIPS PUB 186-3 (using the curves with 256 and 384-bit prime moduli)

Hashing:
Secure Hash Algorithm (SHA) - FIPS PUB 180-3 (using SHA-256 and SHA-384)
Intellectual Property issues have been cited in regards to the adoption of ECC. To mitigate these issues NSA has stated:
(http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml)
A key aspect of Suite B Cryptography is its use of elliptic curve technology instead of classic public key technology. In order to facilitate adoption of Suite B by industry, NSA has licensed the rights to 26 patents held by Certicom, Inc. covering a variety of elliptic curve technology. Under the license, NSA has the right to grant a sublicense to vendors building certain types of products or components that can be used for protecting national security information.
See www.nsa.gov/ia/contacts/index.shtml for more information.
Questions arising from considering this license for Smart Grid use include:

1) Vendors wishing to develop Suite B-enabled commercial-off-the-shelf (COTS) products for use within the field of use of national security need clarification on whether their products are licensable within the field of use.
2) What specific techniques within Suite B are covered by the Certicom license?

3) To what degree can the NSA license be applied to the Smart Grid?
4) What are the licensing terms of this technology outside the NSA sublicense?

These industry issues have resulted in:

1) Technology vendors deploying ECC schemes based on divergent standardization efforts or proprietary specifications that are thwarting interoperability.
2) Technology vendors are avoiding deployment of the standardized techniques thwarting adoption and availability of commercial products.
3) New standardization efforts creating interoperability issues.

It is also worth noting that ECC implementation strategies based on the fundamental algorithms of ECC, which were published prior to the filing dates of many of the patents in this area, are identified and described in:

http://tools.ietf.org/html/draft-mcgrew-fundamental-ecc-01.txt

IPR statements and FAQ covering pricing have been made concerning some commercial use of patented ECC technology:

http://www.certicom.com/images/pdfs/certicom%20-ipr-contribution-to-ietfsept08.pdf
http://www.certicom.com/images/pdfs/certicom%20zigbee%20smart%20energy%20faq_30_mar_2009.pdf

However these have not been comprehensive enough to cover the envisioned scenarios that arise in the Smart Grid. Interoperability efforts, where a small set of core cryptographic techniques are standardized, like NSA's Cryptographic Interoperability Strategy, have been highly effective in building out multi-vendor infrastructures that span numerous standards development organizations' specifications.

Federal support and action that specifies and makes available technology for the Smart Energy infrastructure, similar to the Suite B support for National Security, would remove many of these issues for the Smart Grid.

Break Glass Authentication

TBD next version

Biometrics

TBD next version

D.5.2 Password Complexity Rules

Password complexity rules are intended to ensure that passwords cannot be guessed or cracked by either online or offline password cracking techniques. Offline password cracking is particularly a risk for field equipment in unmanned substations or on pole-tops where the equipment is vulnerable to physical attack that could result in extraction of password hash databases, and for unencrypted communications to field equipment where password hashes could be intercepted.

Incompatible password complexity requirements can make reuse of a password across two different systems impossible. This can improve security since compromise of the password from one system will not result in compromise of password of the other system. Incompatible password complexity requirements might be desirable to force users to choose different passwords for systems with different security levels, e.g., corporate desktop vs. control system. However, forcing users to use too many different passwords can cause higher rates of forgotten passwords and lead users to write passwords down, thereby reducing security. Due to the large number of systems that utility engineers may need access to, reuse of passwords across multiple systems may be necessary. Incompatible password complexity requirements can also cause interoperability problems and make centralized management of passwords for different systems impossible. NIST SP800-63 contains some guidance on measuring password strength and recommendations for minimum password strengths.

Some considerations for password complexity rules follow.

1. Are the requirements based on a commonly recognized standard?
2. Are the requirements strong enough to measurably increase the effort required to crack passwords that meet the rules?
3. Are there hard constraints in the requirements (e.g. minimum and maximum lengths, min and max upper and lowercase, etc.) or soft constraints that simply measure password strength?
4. Are any hard constraints "upper bounds" that can make selecting a password that meets two or more different complexity requirement sets impossible? For example, “must start with a number” and “must start with a letter” are irreconcilable requirements, whereas “must contain a number” and “must contain a letter” do not conflict.
5. Are there alternatives to password complexity rules, such as running password cracking programs on passwords as they are chosen, or two-factor authentication, that can significantly increase security over that provided by password complexity rules, while minimizing user burden?

D.5.3 Authentication

The initial release of the NERC CIP standards did not require strong authentication. In accepting that version of the standards, FERC Order 706 requested NERC to incorporate strong authentication into a future version of the standards.

During the drafting of IEEE-1686, the IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, an effort was made to incorporate strong authentication. The best source of information on strong authentication was found to be NIST SP 800-63, but the format of that document was found unsuitable as a normative reference for an IEEE standard. However, the technical material in NIST SP 800-63 provides some useful advantages for the following reasons:

- The NERC CIP standards are moving from a concept of critical and non-critical assets to three levels of impact: High, Medium, Low

- NIST SP 800-63 provides four levels of authentication assurance, potentially mappable to both the NERC CIP impact levels and the similar approach being taken in the High Level Requirements of this NISTIR
- NIST SP 800-63 provides a framework of requirements but is not overly prescriptive regarding implementation.
- The multi-level approach taken in NIST SP 800-63 is compatible with similar approaches previously taken in guidelines produced for the Bulk Electric System by the NERC Control Systems Security Working Group.

NIST SP 800-63 is a performance specification with four levels of authentication assurance, selectable to match risk. The alternative levels range from Level 1, that allows a simple user ID and password, to Level 4 that is "intended to provide the highest practical remote network authentication assurance". Multi-factor authentication is required at Levels 3 and 4. The NIST document grades the levels in terms of protection against increasingly sophisticated attacks.

D.5.4 Network Access Authentication and Access Control

Several link-layer and network-layer protocols provide network access authentication using EAP (Extensible Authentication Protocol) [RFC3748]. EAP supports a number of authentication algorithms so called EAP methods.

Currently EAP-TLS [RFC5216] and EAP-GPSK [RFC5433] are the IETF Standard Track EAP methods generating key material and supporting mutual authentication. EAP can also be used to provide a key hierarchy to allow confidentiality and integrity protection to be applied to link layer frames.

EAP IEEE 802.1X [802.1X] provides port access control and transports EAP over Ethernet and Wi-Fi. In WiMAX, PKMv2 (Privacy Key Management version 2) in IEEE 802.16e [802.16e] transports EAP. PANA (Protocol for carrying Authentication for Network Access) [RFC5191] transports EAP over UDP/IP. TNP (Trusted Network Connect) [TNC] is an open architecture to enable network operators to enforce policies regarding endpoint integrity using the above mentioned link-layer technologies. There are also ongoing efforts in ZigBee Alliance [ZigBee] to define a network access authentication mechanism for ZigBee Smart Energy 2.0.
In a large-scale deployment, EAP is typically used in pass-through mode where an EAP server is separated from EAP authenticators, and an AAA (Authentication, Authorzation and Accounting) protocol such as RADIUS [RFC2865] is used by a pass-through EAP authenticator for forwarding EAP messages back and forth between an EAP peer to the EAP server. The pass-through authenticator mode introduces a three-party key management, and a number of security considerations so called EAP key management framework [RFC5247] have been made. If an AMI network makes use of EAP for enabling confidentiality and integrity protection at link-layer, it is expected to follow the EAP key management framework.

REFERENCES

[RFC3748] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extensible Authentication Protocol (EAP)", http://www.ietf.org/rfc/rfc3748.txt, June 2004.

[RFC5216] D. Simon, B. Aboba and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, http://www.ietf.org/rfc/rfc5216.txt, March 2008.

[RFC5433] T. Clancy and H. Tschofenig, "Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method", http://www.ietf.org/rfc/rfc5433.txt, February 2009.

[802.1X] IEEE standard for local and metropolitan area networks — port based network access control, IEEE Std 802.1X-2004, December 2004.

[802.16e] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Std 802.16e-2005 and IEEE Std 802.16^(TM)-2004/Cor1-2005, February 2006.

[RFC5191] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", http://www.ietf.org/rfc/rfc5191.txt, May 2008.

[TNC] http://www.trustedcomputinggroup.org/developers/trusted_network_connect

[ZigBee] http://www.zigbee.org/

[RFC2865] Rigney C, Willens S, Rubens A and Simpson W, "Remote authentication dial in user service (RADIUS)", RFC 2865, http://www.ietf.org/rfc/rfc2865.txt, June 2000.

[RFC5247] B. Aboba, D. Simon and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, http://www.ietf.org/rfc/rfc5247.txt, August 2008.

[LiuNing] Donggang Liu, Peng Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), pages 52--61, Washington D.C., October, 2003.

[IOActive] Katie Fehrenbacher "Smart Meter Worm Could Spread Like a Virus", http://earth2tech.com/2009/07/31/smart-meter-worm-could-spread-like-a-virus/.

APPENDIX E
STATE LAWS – SMART GRID AND ELECTRICITY DELIVERY REGULATIONS

This is a non-exhaustive list of State laws and regulations associated with the electric sector. It is hoped that this list will provide a good starting point for those looking for laws applicable in particular states.

State	Code Topic and Links
Alabama	Title 37 Public Utilities Private Contractor providing electricity service Section 37-4-30, Electric cooperatives empowered to furnish telephone service. Section 37-6-41, Cooperatives authorized to supply electrical energy or telephone service or both. Section 37-6-45 http://www.legislature.state.al.us/CodeofAlabama/1975/coatoc.htm
Alaska	No information at this time.
Arizona	42-5063 Definition of Utility - Providing to retail electric customers ancillary services, electric distribution services, electric generation services, electric transmission services and other services related to providing electricity. Customer Protection against unfair and deceptive practices. It has very good consumer protection language http://law.justia.com/arizona/codes/title30/00806.html Statute 30-803 Competition in retail supply of electricity; open markets http://law.justia.com/arizona/codes/title30/00803.html
Arkansas	No information at this time.
California	General Provisions and Definitions http://law.justia.com/california/codes/puc/201-248.html Independent System Operator http://law.justia.com/california/codes/puc/345-352.7.html Distributed Energy Resources http://law.justia.com/california/codes/puc/353.1-353.15.html Privacy Protection of customer data http://law.justia.com/california/codes/puc/2891-2894.10.html
Colorado	Article 25 Public Utility Commission Power to regulate utilities http://law.justia.com/colorado/constitution/cnart25.html
Connecticut	Chapter 98 http://search.cga.state.ct.us/dtsearch_pub_statutes.html

State	Code Topic and Links
	Sec. 7-148ee. Establishment of corporation to manufacture, distribute, purchase or sell electricity, gas or water. Chapter 101 http://search.cga.state.ct.us/dtsearch_pub_statutes.html Municipal Gas and Electric Plant All regulatory measures under Chapter 101 http://search.cga.state.ct.us/dtsearch_pub_statutes.html
Delaware	Title 26 Public Utilities http://delcode.delaware.gov/title26/index.shtml#TopOfPage
District of Columbia	Title 34
Florida	Title 27 Regulated Utilities http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=Ch0350/titl0350.htm&StatuteYear=2009&Title=-%3E2009-%3EChapter%20350 Chapter 366 http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=Ch0366/titl0366.htm&StatuteYear=2009&Title=-%3E2009-%3EChapter%20366
Georgia	Article 2, 6 http://www.lexis-nexis.com/hottopics/gacode/default.asp
Hawaii	http://www.capitol.hawaii.gov/site1/hrs/searchhrs.asp?query=public+utility&currpage=1 §269-16 Regulation of utility rates; ratemaking procedures. http://www.capitol.hawaii.gov/hrscurrent/Vol05_Ch0261-0319/HRS0269/HRS_0269-0016.htm
Idaho	Title 61 http://www.legislature.idaho.gov/idstat/Title61/T61.htm
Illinois	Chapter 220 http://www.ilga.gov/legislation/ilcs/ilcs2.asp?ChapterID=23
Indiana	Title 8 http://www.in.gov/legislative/ic/code/title8/
Iowa	No information at this time.
Kansas	Chapter 66-101 http://www.kslegislature.org/legsrv-statutes/statutesList.do 66-1901-66-1903 http://www.kslegislature.org/legsrv-statutes/statutesList.do
Kentucky	Title 24 Public Utilities Generally http://www.lrc.ky.gov/KRS/278-00/CHAPTER.HTM

State	Code Topic and Links
Louisiana	Louisiana Public Utilities Definition http://www.legis.state.la.us/lss/lss.asp?doc=99873 http://www.legis.state.la.us/lss/lss.asp?doc=99891, http://www.legis.state.la.us/lss/lss.asp?doc=99803, http://www.legis.state.la.us/lss/lss.asp?doc=104770
Maine	Public Utilities http://www.mainelegislature.org/legis/statutes/35/title35ch0sec0.html
Maryland	Statute 1-101 Definitions http://mlis.state.md.us/asp/statutes_Respond2.asp?article=gpu&section=1-101
Massachusetts	No information at this time.
Michigan	Chapter 460 http://www.legislature.mi.gov/%28S%28dlr2op45qzqa4jeojatzee55%29%29/mileg.aspx?page=GetObject&objectname=mcl-chap460
Minnesota	Chapter 216-217 https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter.php?year=2006&start=216&close=217&history=&border=0 Chapter 453 Municipal Electric Power https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter.php?year=2006&start=216&close=217&history=&border=0 Chapter 455 Electric Light and Power Plants https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter_toc.php?year=2006&chapter=455&history=&border=0
Mississippi	No information at this time.
Missouri	No information at this time.
Montana	Title 69 Public Utilities and Carriers https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter_toc.php?year=2006&chapter=455&history=&border=0 Title 69 Chapter 3 Regulation of Public Utilities http://data.opi.state.mt.us/bills/mca_toc/69_3.htm

State	Code Topic and Links
Nebraska	No information at this time.
Nevada	Title 58 Chapter 701 http://www.leg.state.nv.us/NRS/NRS-701.html Renewable Energy Program http://www.leg.state.nv.us/NRS/NRS-701B.html Chapter 703 Public Utility Commission http://www.leg.state.nv.us/NRS/NRS-703.html Regulation of Public Utilities http://www.leg.state.nv.us/NRS/NRS-704.html Utilities Owned by Local Government http://www.leg.state.nv.us/NRS/NRS-710.html
New Hampshire	Statutes http://www.gencourt.state.nh.us/rsa/html/indexes/indexresults.asp Definitions http://www.gencourt.state.nh.us/rsa/html/xxxiv/374-a/374-a-1.htm Private Generation and Sell of Electricity http://www.gencourt.state.nh.us/rsa/html/xxxiv/362-a/362-a-2-a.htm Customer Defined http://www.gencourt.state.nh.us/rsa/html/xxxiv/378/378-7-c.htm Public Utility Defined http://www.gencourt.state.nh.us/rsa/html/xxxiv/362/362-2.htm
New Jersey	No information at this time.
New Mexico	No information at this time.
New York	Electric Utility Cooperatives and Corporations http://public.leginfo.state.ny.us/menugetf.cgi?COMMONQUERY=LAWS Title 2 Article 5 Public Utility Commission http://public.leginfo.state.ny.us/menugetf.cgi?COMMONQUERY=LAWS
North Carolina	No information at this time.
North Dakota	Title 49 Public Utilities http://www.legis.nd.gov/cencode/t49.html
Ohio	Chapter 49 Utilities – Electric; Gas; Water http://codes.ohio.gov/orc/49 Chapter 743 Municipal Utilities http://codes.ohio.gov/orc/743
Oklahoma	No information at this time.
Oregon	Title 57 Utility Regulation http://www.leg.state.or.us/ors/756.html
Pennsylvania	Title 66
Rhode Island	Title 39 Public Utilities and Carriers http://www.rilin.state.ri.us/Statutes/TITLE39/INDEX.HTM

State	Code Topic and Links
South Carolina	Article 3 Electric Systems http://www.scstatehouse.gov/coderegs/c103.htm
South Dakota	Title 49 Public Utilities and Carriers http://legis.state.sd.us/statutes/DisplayStatute.aspx?Type=Statute&Statute=49
Tennessee	Title 65 Chapter 4 Public Utility Commission Authority http://michie.lexisnexis.com/tennessee/lpext.dll/tncode/270f1/272b2?fn=document-frame.htm&f=templates&2.0# Chapter 34 Territories of Electric Utility Systems http://michie.lexisnexis.com/tennessee/lpext.dll/tncode/270f1/27d62?f=templates&fn=document-frame.htm&2.0#JD_t65ch34 Chapter 23 State Rural Electrification Authority http://michie.lexisnexis.com/tennessee/lpext.dll/tncode/270f1/27985?f=templates&fn=document-frame.htm&2.0#JD_t65ch23
Texas	Utilities Code Title 2 Public Utility Regulatory Act Subtitle Electric Utilities Chapter 31 General Provisions http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.31.htm Chapter 38 Regulation http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.38.htm Chapter 39 Restructuring http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.39.htm Chapter 40 Publicly Owned http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.40.htm Chapter 41 Cooperatives http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.41.htm Chapter 43 Access to Broadband http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.43.htm
Utah	Title 54 Public Utilities http://le.utah.gov/~code/TITLE54/TITLE54.htm
Vermont	No information at this time.
Virginia	Title 56 Section 580 Transmission and distribution of electricity http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+56-580 Definitions http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+56-265.1
Washington	Title 54 http://apps.leg.wa.gov/rcw/default.aspx?Cite=54 Electric Power http://apps.leg.wa.gov/rcw/default.aspx?cite=54.44
West Virginia	No information at this time.
Wisconsin	Chapter 196 Regulation of Public Utilities http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=index&jd=top

State	Code Topic and Links
	Utility service for persons who are victims of Identity Theft http://www.legis.state.wi.us/statutes/Stat0196.pdf
Wyoming	Title 37 Public Utilities

APPENDIX F
GLOSSARY AND ACRONYMS

Aggregation	Practice of summarizing certain data and presenting it as a total without any PII identifiers
AICPA	American Institute of Certified Public Accountants. The national, professional organization for all Certified Public Accountants.
AMI	Advanced Metering Infrastructure
Anonymize	A process of transformation or elimination of PII for purposes of sharing data
ASAP-SG	Advanced Security Acceleration Project-Smart Grid
B2B	Business to Business
BAN	Business Area Network
CIM	Common Information Model. A structured set of definitions that allow different Smart Grid domain representatives to communicate important concepts and exchange information easily and effectively.
CIP	Critical Infrastructure Protection
CSWG	Cyber Security Working Group
DA	Distribution Automation
De-identify	A form of anonymization that does not attempt to control the data once it has had PII identifiers removed, so it is at risk of re-identification.
DER	Distributed Energy Resources
DHS	Department of Homeland Security
DMS	Distribution Management System
DNP	Distributed Network Protocol
DOE	Department of Energy
DOMA	Distribution Operations Model and Analysis
DR	Demand Response
EMS	Energy Management System
EPRI	Electric Power Research Institute
ES	Electric Storage
ESI	Energy Services Interface
ET	Electric Transportation
EUMD	End Use Measurement Device

EV/PHEV	Electric Vehicle/Plug-in Hybrid Electric Vehicles. Cars or other vehicles that draw electricity from batteries to power an electric motor. PHEVs also contain an internal combustion engine.
EVSE	Electric Vehicle Service Element
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standard Document
FLIR	Fault Location, Isolation, Restoration
G&T	Generations and Transmission
GAPP	Generally Accepted Privacy Principles. Privacy principles and criteria developed and updated by the AICPA and Canadian Institute of Chartered Accountants to assist organizations in the design and implementation of sound privacy practices and policies.
GIS	Geographic Information System
GRPS	General Packet Radio Service
HAN	Home Area Network. A network of energy management devices, digital consumer electronics, signal-controlled or enabled appliances, and applications within a home environment that is on the home side of the electric meter.
HMI	Human-Machine Interface
I2G	Industry to Grid
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
ISA	International Society of Automation
ISO	Independent System Operator
ISO/IEC27001	International Organization for Standardization/International Electrotechnical Commission Standard 27001. A auditable international standard that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It uses a process approach for protection of critical information.
IT	Information Technology
LAN	Local Area Network
LMS/DRMS	Load Management System/ Distribution Resource Management System
MDMS	Meter Data Management System

MFR	Multi-Feeder Reconnection
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OECD	Organisation for Economic Cooperation and Development. A global governmental forum of 30+ market democracies for comparison of policy experiences, good practices, and coordination of domestic and international policies. It is one of the world's largest and most reliable sources of comparable statistical, economic and social data.
OMS	Outage Management System
OWASP	Open Web Application Security Project
PAP	Priority Action Plan
Personal Information	Information that reveals details, either explicitly or implicitly, about a specific individual's household dwelling or other type of premises. This is expanded beyond the normal "individual" component because there are serious privacy impacts for all individuals living in one dwelling or premise. This can include items such as energy use patterns or other types of activities. The pattern can become unique to a household or premises just as a fingerprint or DNA is unique to an individual.
PEV	Plug-In Electric Vehicle
PI	Process Information
PIA	Privacy Impact Assessment. A process used to evaluate the possible privacy risks to personal information, in all forms, collected, transmitted, shared, stored, disposed of, and accessed in any other way, along with the mitigation of those risks at the beginning of and throughout the life cycle of the associated process, program or system.
PII	Personally Identifying Information
R&D	Research and Development
RTO	Regional Transmission Operator
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SGIP	Smart Grid Interoperability Panel
SGIP-CSWG	SGIP – Cyber Security Working Group
SP	Special Publication
SSP	Sector-specific Plans

VVWS	Volt-Var-Watt
WAMS	Wide-Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WLAN	Wireless Local Area Network
WMS	Work Management System

APPENDIX G
SGIP-CSWG MEMBERSHIP

This list is all participants in the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG), formerly the Cyber Security Coordination Task Group (CSCTG), and all of the sub-groups.

	Name	Organization
1.	Ackerman, Eric	Edison Electric Institute
2.	Akyol, Bora	Pacific Northwest National Laboratory
3.	Alexander, Roger	Eka Systems, Inc.
4.	Alrich, Tom	ENCARI
5.	Ambady, Balu	Sensus
6.	Anderson, Dwight	Schweitzer Engineering Labs
7.	Ascough, Jessica	Harris Corporation
8.	Bacik, Sandy	Enernex
9.	Baiba Grazdina	Duke Energy
10.	Barclay, Steve	ATIS
11.	Barnes, Frank	University of Colorado at Boulder
12.	Barnett, Bruce	GE Global Research
13.	Barr, Michael	L-3 Communications Nova Engineering
14.	Bass, Len	Software Engineering Institute, Carnegie Mellon University
15.	Batz, David	Edison Electric Institute
16.	Bell, Ray	Grid Net
17.	Bell, Will	Grid Net
18.	Bender, Klaus	Utilities Telecom Council
19.	Benn, Jason	Hawaiian Electric Company
20.	Bennett, Bob	Xcel Energy
21.	Berkowitz, Don	S&C Electric Company
22.	Beroset, Ed	Elster Group
23.	Berrett, Dan E.	DHS Standards Awareness Team (SAT)
24.	Berrey, Adam	General Catalyst Partners
25.	Bhaskar, Mithun M.	National Institute of Technology, Warangal
26.	Biggs, Doug	Infogard
27.	Biggs, Les	Infogard
28.	Blomgren, Paul	SafeNet Inc.
29.	Bochman, Andy	
30.	Braendle, Markus	ABB
31.	Branco, Carlos	Northeast Utilities
32.	Brewer, Tanya	NIST

	Name	Organization
33.	Brigati, David	NitroSecurity
34.	Brown, Bobby	EnerNex Corporation
35.	Brozek, Mike	Westar Energy, Inc.
36.	Bucciero, Joe	Buccerio Consulting
37.	Burnham, Laurie	Dartmouth College
38.	Butterworth, Jim	Guidance Software
39.	Camilleri, John	Green Energy Corp
40.	Campagna, Matt	Certicom Corp.
41.	Cam-Winget, Nancy	Cisco Systems, Inc.
42.	Caprio, Daniel	McKenna Long & Aldridge LLP
43.	Cardenas, Alvaro A.	Fujitsu
44.	Carlson, Chris	Puget Sound Energy
45.	Carpenter, Matthew	InGuardians
46.	Chaney, Mike	Securicon
47.	Chasko, Stephen	Landis+Gyr
48.	Chow, Edward	U of Colorado at Colorado Springs
49.	Cioni, Mark V.	MV Cioni Associates, Inc.
50.	Clements, Sam	Pacific Northwest National Laboratory
51.	Cleveland, Frances	Xanthus Consulting International
52.	Cohen, Mike	Mitre
53.	Coney, Lillie	Electronic Privacy Information Center
54.	Coop, Mike	heyCoop, LLC
55.	Cornish, Kevin	Enspiria
56.	Cortes, Sarah	Inman Technology IT
57.	Cosio, George	Florida Power and Light
58.	Cragie, Robert	Jennic LTD
59.	Crane, Melissa	Tennessee Valley Authority
60.	Cui, Stephen	Microchip Technology
61.	Dagle, Jeff	Pacific Northwest National Laboratory
62.	Dalva, Dave	Cisco Systems, Inc.
63.	Danahy, Jack	Bochman & Danahy Research
64.	Dangler, Jack	SAIC
65.	De Petrillo, Nick	Industrial Defender
66.	di Sabato, Mark	
67.	Dillon, Terry	APS
68.	Dinges, Sharon	Trane
69.	Dion, Thomas	Dept of Homeland Security
70.	Dodson, Greg	Dominion Resources Services, Inc.
71.	Doreswamy, Rangan	
72.	Dorn, John	Accenture

	Name	Organization
73.	Downum, Wesley	Telcordia
74.	Dransfield, Michael	National Security Agency
75.	Drozinski, Timothy	Florida Power & Light Company
76.	Drummond, Rik	Drummond Group
77.	Dubrawsky, Ido	Itron
78.	Dupper, Jeff	Ball Aerospace & Technologies
79.	Duren, Michael	Protected Computing
80.	Dutta, Prosenjit	Utilities AMI Practice
81.	Earl, Frank	Earl Consulting
82.	Eastham, Bryant	Panasonic Electric Works Laboratory of America (PEWLA)
83.	Edgar, Tom	Pacific Northwest National Laboratory
84.	Eggers, Matthew	U.S. Chamber of Commerce
85.	Eigenhuis, Scott M	Accenture
86.	Emelko, Glenn	ESCO
87.	Engels, Mark	Dominion Resources Services, Inc.
88.	Ennis, Greg	Wi-Fi Alliance
89.	Enstrom, Mark	NeuStar
90.	Eraker, Liz	Samuelson Clinic at UC Berkeley
91.	Estefania, Maria	ATIS
92.	Eswarahally, Shrinath	Infineon Technologies NA
93.	Ewing, Chris	Schweitzer Engineering Labs
94.	Fabela, Ronnie	Lockheed Martin
95.	Faith, Doug	MW Consulting
96.	Faith, Nathan	American Electric Power
97.	Famolari, David	Telcordia Technologies
98.	Fennell, Kevin	Landis+Gyr
99.	Fisher, Jim	Noblis
100.	Fishman, Aryah	Edison Electric Institute
101.	Franz, Matthew	SAIC
102.	Fredebeil, Karlton	Tennessee Valley Authority
103.	Freund, Mark	Pacific Gas and Electric Company
104.	Fuloria, Shailendra	Cambridge University
105.	Gailey, Mike	CSC
106.	Garrard, Ken	Aunigma Network Solutions Corp.
107.	Gerber, Josh	San Diego Gas and Electric
108.	Gerbino, Nick	Dominion Resources Services, Inc.
109.	Gering, Kip	Itron
110.	Gerra, Arun	University of Colorado, Boulder
111.	Ghansah, Isaac	California State University Sacramento

	Name	Organization
112.	Giammaria, Claire	American Civil Liberties Union
113.	Gibbs, Derek	SmartSynch
114.	Gillmore, Matt	CMS Energy
115.	Givens, Beth	Privacy Rights Clearinghouse
116.	Glenn, Bill	Westar Energy, Inc.
117.	Goff, Ed	Progress Energy
118.	Golla, Ramprasad	Grid Net
119.	Gonzalez, Efrain	Southern California Edison
120.	Gooding, Jeff	Southern California Edison
121.	Goodson, Paul	ISA
122.	Gorog, Christopher	Atmel Corporation
123.	Grazdina, Baiba	Duke Energy
124.	Greenberg, Alan M.	Boeing Defense, Space & Security
125.	Greenfield, Neil	American Electric Power, Inc.
126.	Greer, David	University of Tulsa
127.	Grochow, Jerrold	MIT
128.	Gulick, Jessica	SAIC
129.	Gunter, Carl	U. of Illinois
130.	Gupta, Rajesh	UC San Diego
131.	Hague, David	
132.	Halbgewachs, Ronald D.	Sandia National Laboratories
133.	Hall, Tim	Mocana
134.	Hallman, Georgia	Guidance Software
135.	Hambrick, Gene	Carnegie Mellon University
136.	Hardjono, Thomas	MIT
137.	He, Donya	BAE Systems
138.	Herold, Rebecca	Privacy Professor Rebecca Herold & Associates, LLC
139.	Heron, George L.	BlueFin Security
140.	Herrell, Jonas	University of California, Berkeley
141.	Hertzog, Christine	Smart Grid Library
142.	Highfill, Darren	SCE
143.	Hilber, Del	Constellation Energy
144.	Histed, Jonathan	Novar | Honeywell
145.	Holstein, Dennis	OPUS Consulting Group
146.	Hoofnagle, Chris	University of California, Berkeley
147.	Houseman, Doug	Capgemini Consulting
148.	Huber, Robert	Critical Intelligence
149.	Hughes, Joe	EPRI
150.	Hurley, Jesse	Shift Research, LLC
151.	Hussey, Laura	Schweitzer Engineering Laboratories, Inc.

	Name	Organization
152.	Huzmezan, Mihai	General Electric
153.	Ibrahim, Erfan	EPRI
154.	Iga, Yoichi	NEC Electronics Corp.
155.	Ilic, Marija	Carnegie-Mellon University
156.	Ivers, James	SEI
157.	Jaokar, Ajit	Futuretext
158.	Jepson, Robert	Lockheed Martin Energy Solutions
159.	Jin, Chunlian	Pacific Northwest National Laboratory
160.	Joffe, Rodney	NeuStar
161.	Johnson, Diana J.	Boeing Defense, Space & Security
162.	Johnson, Freemon	NIST
163.	Johnson, Oliver	Tendril
164.	Jones, Barry	Sempra
165.	Kahl, Steve	North Dakota
166.	Kanda, Mitsuru	Toshiba
167.	Kellogg, Shannon	EMC
168.	Kenchington, Henry	DOE
169.	Kerber, Jennifer	Tech America
170.	Khurana, Himanshu	University of Illinois
171.	Kim, Jin	Risk Networks LLC
172.	Kimura, Randy	General Electric
173.	King, Charlie	BAE Systems
174.	Kirby, Bill	Aunigma Network Solutions Corp.
175.	Kiss, Gabor	Telcordia
176.	Klein, Stanley A.	Open Secure Energy Control Systems, LLC
177.	Klerer, Mark	
178.	Kobayashi, Nobuhiro	Mitsubishi Electric
179.	Koliwad, Ajay	General Electric
180.	Kotting, Chris	Public Utilities Commission of Ohio
181.	Kube, Nate	Wurldtech
182.	Kulkarni, Manoj	Mocana
183.	Kursawe, Klaus	Philips
184.	Kuruganti, Phani Teja	EMC2
185.	Kyle, Martin	Sierra Systems
186.	Lakshminarayanan, Sitaraman	General Electric
187.	LaMarre, Mike	Austin Energy ITT
188.	Lauriat, Nicholas A.	Network and Security Technologies
189.	Lawson, Barry	NRECA
190.	Lee, Annabelle	NIST

	Name	Organization
191.	Lee, Cheolwon	Electronics and Telecommunications Research Institute
192.	Lee, Gunhee	Electronics and Telecommunications Research Institute
193.	Lee, JJ	LS Industrial Systems
194.	Lee, Virginia	eComp Consultants
195.	Lenane, Brian	SRA International
196.	Levinson, Alex	Lockheed Martin Information Systems and Global Solutions
197.	Lewis, David	Hydro One
198.	Lewis, Rob	Trustifiers Inc.
199.	Libous, Jim	Lockheed Martin Systems Integration – Owego
200.	Lilley, John	Sempra
201.	Lima, Claudio	Sonoma Innovation
202.	Lintzen, Johannes	Utimaco Safeware AG
203.	Lipson, Howard	CERT, Software Engineering Institute
204.	Lynch, Jennifer	University of California, Berkeley
205.	Maciel, Greg	Uniloc USA
206.	Magda, Wally	Industrial Defender
207.	Magnuson, Gail	
208.	Manjrekar, Madhav	Siemens
209.	Manucharyan, Hovanes	LinkGard Systems
210.	Maria, Art	AT&T
211.	Markham, Tom	Honeywell
212.	Martinez, Catherine	DTE Energy
213.	Martinez, Ralph	BAE Systems
214.	Marty, David	University of California, Berkeley
215.	McBride, Sean	Critical Intelligence
216.	McComber, Robert	Telvent
217.	McCullough, Jeff	Elster Group
218.	McDonald, Jeremy	Southern California Edison
219.	McGinnis, Douglas	IT Utility Solutions
220.	McGurk, Sean	Dept of Homeland Security
221.	McKinnon, David	Pacific Northwest National Laboratory
222.	McQuade, Rae	NAESB
223.	Melton, Ron	Pacific Northwest National Laboratory
224.	Mertz, Michael	Southern California Edison
225.	Metke, Anthony	Motorola
226.	Miller, Joel	Merrion Group
227.	Mirza, Wasi	Motorola

	Name	Organization
228.	Mitsuru, Kanda	Toshiba
229.	Molina, Jesus	Fujitsu Ltd.
230.	Molitor, Paul	NEMA
231.	Mollenkopf, Jim	CURRENT Group
232.	Moniz, Paulo	Logica
233.	Mulberry, Karen	Neustar
234.	Nahas, John	ICF International
235.	Navid, Nivad	Midwest ISO
236.	Noel, Paul	ASI
237.	Norton, Dave	Entergy
238.	Nutaro, James J.	Southern California Edison
239.	O'Neill, Ivan	Southern California Edison
240.	Ohba, Yoshihiro	Toshiba
241.	Okunami, Peter M.	Hawaiian Electric Company, Inc.
242.	Old, Robert	Siemens Building Technologies, Inc.
243.	Olive, Kay	Olive Strategies
244.	Overman, Thomas M.	Boeing Defense, Space & Security
245.	Owens, Andy	Plexus Research
246.	Pace, James	Silver Spring Networks
247.	Pal, Partha	Raytheon BBN Technologies
248.	Palmquist, Scott	Itron
249.	Papa, Mauricio	University of Tulsa
250.	Patel, Chris	EMC Technology Alliances
251.	Pearce, Thomas C. II	Public Utilities Commission of Ohio
252.	Peters, Mike	FERC
253.	Phillips, Matthew	Electronic Privacy Information Center
254.	Phillips, Michael	Centerpoint Energy
255.	Phiri, Lindani	Elster Group
256.	Polonetsky, Jules	The Future of Privacy Forum
257.	Powell, Terry	L-3 Communications
258.	Puri, Anuj	IEEE
259.	Pyles, Ward	Southern Company
260.	Qin, Jason	Skywise Systems
261.	Qiu, Bin	E:SO Global
262.	Quinn, Steve	Sophos
263.	Rader, Bodhi	FERC
264.	Radgowski, John	Dominion Resources Services, Inc
265.	Ragsdale, Gary L.	Southwest Research Institute
266.	Rakaczky, Ernest A.	Invensys Global Development
267.	Rao, Josyula R	IBM

	Name	Organization
268.	Ray, Indrakshi	Colorado State University
269.	Reddi, Ramesh	Intell Energy
270.	Revill, David	Georgia Transmission Corp.
271.	Rick Schantz	BBN
272.	Riepenkroger, Karen	Sprint
273.	Rivero, Al	Telvent
274.	Roberts, Don	Southern Company Transmission
275.	Roberts, Jeremy	LonMark International
276.	Robinson, Charley	International Society of Automation
277.	Robinson, Eric	ITRON
278.	Rodriguez, Gene	IBM
279.	Rumery, Brad	Sempra
280.	Rutfield, Craig	NTRU Cryptosystems, Inc.
281.	Rutkowski, Tony	Yaana Technologies
282.	Sackman, Ronald W.	Boeing Defense, Space & Security
283.	Saint, Bob	National Rural Electric Cooperative Association
284.	Sambasivan, Sam	AT&T
285.	Sanders, William	University of Illinois
286.	Schantz, Rick	Raytheon BBN Technologies
287.	Scheff, Andrew	Scheff Associates
288.	Sconzo, Mike	Electric Reliability Council of Texas
289.	Scott, David	IEEE
290.	Scott, Tom	Progress Energy
291.	Searle, Justin	InGuardians
292.	Seo, Jeongtaek	Electronics and Telecommunications Research Institute
293.	Shastri, Viji	MCAP Systems
294.	Shaw, Vishant	Enernex
295.	Shein, Robert	EDS
296.	Shetty, Ram	General Electric
297.	Shin, Mark	Infogard
298.	Shpantzer, Gal	
299.	Silverstone, Ariel	Independent Business Security Consultant
300.	Sinai, Nick	Federal Communications Commission
301.	Singer, Bryan	Kenexis
302.	Sisley, Elizabeth	University of Minnesota
303.	Skare, Paul	Siemens
304.	Slack, Phil	Florida Power & Light Company
305.	Smith, Brian	EnerNex
306.	Smith, Rhett	Schweitzer Engineering Laboratories, Inc.

	Name	Organization
307.	Smith, Ron	ESCO Technologies Inc.
308.	Sood, Kapil	Intel Labs
309.	Sorebo, Gilbert	SAIC
310.	Souza, Bill	GridWise and PJM Interconnection
311.	Stammberger, Kurt	Mocana
312.	Stanley, Jay	American Civil Liberties Union
313.	Starr, Christopher H.	General Dynamics Advanced Information Systems
314.	Steiner, Michael	IBM
315.	Sterling, Joyce	NitroSecurity
316.	Stevens, James	Software Engineering Institute
317.	Stitzel, Jon	Burns & McDonnell Engineering Company, Inc.
318.	StJohns, Michael	
319.	Stouffer, Keith	NIST
320.	Strickland, Tom	General Electric
321.	Struthers, Brent	NeuStar
322.	Subrahmanyam. P.A.	IEEE, Stanford, CyberKnowledge
323.	Suchman, Bonnie	Troutman Sanders LLP
324.	Sullivan, Kevin	Microsoft
325.	Sung, Lee	Fujitsu
326.	Sushilendra, Madhava	EPRI
327.	Tallent, Michael	Tennessee Valley Authority
328.	Taylor, Malcolm	Carnegie Mellon University
329.	Thanos, Daniel	General Electric
330.	Thaw, David	Hogan & Hartson
331.	Thomassen, Tom	Symantec
332.	Thompson, Daryl L.	Thompson Network Consulting
333.	Thomson, Matt	General Electric
334.	Tien, Lee	Electronic Freedom Foundation
335.	Tiffany, Eric	Liberty Alliance
336.	Toecker, Michael	Burns & McDonnell
337.	Tolway, Rich	APS
338.	Truskowski, Mike	Cisco
339.	Uhrig, Rick	Electrosoft
340.	Urban, Jennifer	Samuelson Clinic at UC Berkeley
341.	Veltsos, Christophe	Minnesota State University
342.	Venkatachalam, R. S.	Mansai Corporation
343.	Vettoretti, Paul	SBC Global
344.	Wacks, Kenneth P.	Massachusetts Institute of Technology
345.	Walia, Harpreet	Wave Strong Inc.
346.	Wallace, Donald	Itron

	Name	Organization
347.	Walters, Ryan	COO TerraWi Communications
348.	Wang, Longhao	Samuelson Clinic at UC Berkeley
349.	Wang, Yongge	University of North Carolina-Charlotte
350.	Wei, Dong	SIEMENS Corporation
351.	Wepman, Joshua	SAIC Commercial Business Services
352.	West, Andrew C	Invensys Process Systems
353.	Weyer, John A.	John A. Weyer and Associates
354.	Whitaker, Kari	LockDown, Inc.
355.	White, Jim	Uniloc USA, Inc.
356.	Whitney, Tobias	The Structure Group
357.	Whyte, William	Ntru Cryptosystems, Inc.
358.	Williams, Terron	Elster Electricity
359.	Wingo, Harry	Google
360.	Witnov, Shane	University of California, Berkeley
361.	Wohnig, Ernest	Booz-Allen Hamilton
362.	Wolf, Dana	RSA
363.	Worden, Michael	New York State Public Service Commission
364.	Worthington, Charles	Federal Communications Commission
365.	Wright, Andrew	N-Dimension Solutions
366.	Wyatt, Michael	ITT Advanced Technologies
367.	Yao, Taketsugu	Oki Electric Industry, Co., Ltd
368.	Yardley, Tim	University of Illinois
369.	Yoo, Kevin	Wurldtech