Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

Series/Number:	NISTIR 7628
Title:	Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements Vol. 2, Privacy and the Smart Grid Vol. 3, Supportive Analyses and References
Publication Date(s):	August 2010
Withdrawal Date:	September 2014
Withdrawal Note:	Replaced by NISTIR 7628 Rev. 1

Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	NISTIR 7628 Rev. 1
Title:	Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements Vol. 2, Privacy and the Smart Grid Vol. 3, Supportive Analyses and References
Author(s):	The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee
Publication Date(s):	September 2014
URL/DOI:	https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

Additional Information (if applicable)

Contact:	Computer Security Division (Information Technology Laboratory)
Latest revision of the attached publication:	NISTIR 7628 Rev. 1 (September 2014)
Related information:	https://csrc.nist.gov/
Withdrawal announcement (link):	N/A

Date updated: June 9, 2015

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

NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

The Smart Grid Interoperability Panel – Cyber Security Working Group

August 2010

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

NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

The Smart Grid Interoperability Panel–Cyber Security Working Group

August 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 (IT). 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 National Institute of Standards and Technology Interagency Report (NISTIR) 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, vol. 1
289 pages (August 2010)

ACKNOWLEDGMENTS

This report was developed by members of the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP-CSWG), formerly the Cyber Security Coordination Task Group (CSCTG), and during its development was chaired by Annabelle Lee of the Federal Energy Regulatory Commission (FERC), formerly of NIST. The CSWG is now chaired by Marianne Swanson (NIST). Alan Greenberg (Boeing), Dave Dalva (Cisco Systems), and Bill Hunteman (Department of Energy) are the vice chairs. Mark Enstrom (Neustar) is the secretary. Tanya Brewer of NIST is the lead editor of this report. The members of the SGIP-CSWG have extensive technical expertise and knowledge to address the cyber security needs of the Smart Grid. The dedication and commitment of all these individuals over the past year and a half is significant. In addition, appreciation is extended to the various organizations that have committed these resources to supporting this endeavor. Members of the SGIP-CSWG and the working groups of the SGIP-CSWG are listed in Appendix J of this report.

In addition, acknowledgement is extended to the NIST Smart Grid Team, consisting of staff in the NIST Smart Grid Office and several of NIST's Laboratories. Under the leadership of Dr. George Arnold, National Coordinator for Smart Grid Interoperability, their ongoing contribution and support of the CSWG efforts have been instrumental to the success of this report.

Additional thanks are extended to Diana Johnson (Boeing) and Liz Lennon (NIST) for their superb technical editing of this report. Their expertise, patience, and dedication were critical in producing a quality report. Thanks are also extended to Victoria Yan (Booz Allen Hamilton). Her enthusiasm and willingness to jump in with both feet are really appreciated.

Finally, acknowledgment is extended to all the other individuals who have contributed their time and knowledge to ensure this report addresses the security needs of the Smart Grid.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The United States has embarked on a major transformation of its electric power infrastructure. This vast infrastructure upgrade—extending from homes and businesses to fossil-fuel-powered generating plants and wind farms, affecting nearly everyone and everything in between—is central to national efforts to increase energy efficiency, reliability, and security; to transition to renewable sources of energy; to reduce greenhouse gas emissions; and to build a sustainable economy that ensures future prosperity. These and other prospective benefits of "smart" electric power grids are being pursued across the globe.

Steps to transform the nation's aging electric power grid into an advanced, digital infrastructure with two-way capabilities for communicating information, controlling equipment, and distributing energy will take place over many years. In concert with these developments and the underpinning public and private investments, key enabling activities also must be accomplished. Chief among them is devising effective strategies for protecting the privacy of Smart Grid-related data and for securing the computing and communication networks that will be central to the performance and availability of the envisioned electric power infrastructure. While integrating information technologies is essential to building the Smart Grid and realizing its benefits, the same networked technologies add complexity and also introduce new interdependencies and vulnerabilities. Approaches to secure these technologies and to protect privacy must be designed and implemented early in the transition to the Smart Grid.

This three-volume report, *Guidelines for Smart Grid Cyber Security*, presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of Smart Grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information presented in this report as guidance for assessing risk and identifying and applying appropriate security requirements. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cyber security requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

This initial version of *Guidelines for Smart Grid Cyber Security* was developed as a consensus document by the Cyber Security Working Group (CSWG) of the Smart Grid Interoperability Panel (SGIP), a public-private partnership launched by the National Institute of Standards and Technology (NIST) in November 2009.[1] The CSWG now numbers more than 475 participants from the private sector (including vendors and service providers), manufacturers, various standards organizations, academia, regulatory organizations, and federal agencies. A number of these members are from outside of the U.S.

[1] For a brief overview of this organization, read the *Smart Grid Interoperability Panel: A New, Open Forum for Standards Collaboration* at: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CMEWG/Whatis_SGIP_final.pdf.

This document is a companion document to the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* (NIST SP 1108),[2] which NIST issued on January 19, 2010. The framework and roadmap report describes a high-level conceptual reference model for the Smart Grid, identifies standards that are applicable (or likely to be applicable) to the ongoing development of an interoperable Smart Grid, and specifies a set of high-priority standards-related gaps and issues. Cyber security is recognized as a critical, cross-cutting issue that must be addressed in all standards developed for Smart Grid applications. Given the transcending importance of cyber security to Smart Grid performance and reliability, this document "drills down" from the initial release of the *NIST Framework and Roadmap*, providing the technical background and additional details that can inform organizations in their risk management efforts to securely implement Smart Grid technologies. The Framework document is the first installment in an ongoing standards and harmonization process. Ultimately, this process will deliver the hundreds of communication protocols, standard interfaces, and other widely accepted and adopted technical specifications necessary to build an advanced, secure electric power grid with two-way communication and control capabilities. The *Guidelines for Smart Grid Cyber Security* expands upon the discussion of cyber security included in the Framework document. The CSWG will continue to provide additional guidance as the Framework document is updated and expanded to address testing and certification, the development of an overall architecture, and as additional standards are identified.

This document is the product of a participatory public process that, starting in March 2009, included workshops as well as weekly teleconferences, all of which were open to all interested parties. Drafts of the three volumes have undergone at least one round of formal public review. Portions of the document have undergone two rounds of review and comment, both announced through notices in the Federal Register.[3]

The three volumes that make up this initial set of guidelines are intended primarily for individuals and organizations responsible for addressing cyber security for Smart Grid systems and the constituent subsystems of hardware and software components. Given the widespread and growing importance of the electric infrastructure in the U.S. economy, these individuals and organizations comprise a large and diverse group. It includes vendors of energy information and management services, equipment manufacturers, utilities, system operators, regulators, researchers, and network specialists. In addition, the guidelines have been drafted to incorporate the perspectives of three primary industries converging on opportunities enabled by the emerging Smart Grid—utilities and other business in the electric power sector, the information technology industry, and the telecommunications sector.

Following this executive summary, the first volume of the report describes the analytical approach, including the risk assessment process, used to identify high-level security requirements. It also presents a high-level architecture followed by a logical interface

[2] Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108)*, Jan. 2010. The report can be downloaded at: http://nist.gov/smartgrid/

[3] 1) *Federal Register*: October 9, 2009 (Volume 74, Number 195) [Notices], pp. 52183-52184; 2) *Federal Register:* April 13, 2010 (Volume 75, Number 70) [Notices], pp. 18819-18823.

architecture used to identify and define categories of interfaces within and across the seven Smart Grid domains. High-level security requirements for each of the 22 logical interface categories are then described. The first volume concludes with a discussion of technical cryptographic and key management issues across the scope of Smart Grid systems and devices.

The second volume is focused on privacy issues within personal dwellings. It provides awareness and discussion of such topics as evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, and their behavior within their premises and electric vehicles; and whether these new types of information may contain privacy risks and challenges that have not been legally tested yet. Additionally, the second volume provides recommendations, based on widely accepted privacy principles, for entities that participate within the Smart Grid. These recommendations include things such as having entities develop privacy use cases that track data flows containing personal information in order to address and mitigate common privacy risks that exist within business processes within the Smart Grid; and to educate consumers and other individuals about the privacy risks within the Smart Grid and what they can do to mitigate these risks.

The third volume is a compilation of supporting analyses and references used to develop the high-level security requirements and other tools and resources presented in the first two volumes. These include categories of vulnerabilities defined by the working group and a discussion of the bottom-up security analysis that it conducted while developing the guidelines. A separate chapter distills research and development themes that are meant to present paradigm changing directions in cyber security that will enable higher levels of reliability and security for the Smart Grid as it continues to become more technologically advanced. In addition, the third volume provides an overview of the process that the CSWG developed to assess whether standards, identified through the NIST-led process in support of Smart Grid interoperability, satisfy the high-level security requirements included in this report.

Beyond this executive summary, it is assumed that readers of this report have a functional knowledge of the electric power grid and a functional understanding of cyber security.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
  - 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* includes a high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. The chapter also includes individual diagrams for each of the 22 logical interface categories. This architecture focuses on a short-term view (1–3 years) of the Smart Grid.

  - Chapter 3 – *High Level Security Requirements* specifies the high level security requirements for the Smart Grid for each of the 22 logical interface categories included in Chapter 2.
  - Chapter 4 – *Cryptography and Key Management* identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.
  - Appendix A – *Crosswalk of Cyber Security Documents*
  - Appendix B – *Example Security Technologies and Procedures to Meet the High Level Security Requirements*
- Volume 2 – Privacy and the Smart Grid
  - Chapter 5 – *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 that may occur as new capabilities are included in the Smart Grid.
  - Appendix C – *State Laws – Smart Grid and Electricity Delivery*
  - Appendix D – *Privacy Use Cases*
  - Appendix E – *Privacy Related Definitions*
- Volume 3 – Supportive Analyses and References
  - Chapter 6 – *Vulnerability Classes* includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.
  - Chapter 7 – *Bottom-Up Security Analysis of the Smart Grid* identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.
  - Chapter 8 – *Research and Development Themes for Cyber Security in the Smart Grid* 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.
  - Chapter 9 – *Overview of the Standards Review* includes an overview of the process that is being used to assess standards against the high level security requirements included in this report.
  - Chapter 10 – *Key Power System Use Cases for Security Requirements* identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.
  - Appendix F – *Logical Architecture and Interfaces of the Smart Grid*
  - Appendix G – *Analysis Matrix of Interface Categories*
  - Appendix H – *Mappings to the High Level Security Requirements*
  - Appendix I – *Glossary and Acronyms*
  - Appendix J – *SGIP-CSWG Membership*

CHAPTER ONE
CYBER SECURITY STRATEGY

With the implementation of the Smart Grid has come an increase in the importance of the information technology (IT) and telecommunications infrastructures in ensuring the reliability and security of the electric sector. Therefore, the security of systems and information in the IT and telecommunications infrastructures must be addressed by an evolving electric sector. Security must be included in all phases of the system development life cycle, from design phase through implementation, maintenance, and disposition/sunset.

Cyber security must address not only deliberate attacks launched by disgruntled employees, agents of 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)[4], the Department of Homeland Security (DHS),[5] the Department of Energy (DOE),[6] and the Federal Energy Regulatory Commission (FERC).[7]

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 the introduction of malicious software/firmware or compromised hardware could result in denial of service (DoS) or other malicious attacks;
- Increased number of entry points and paths are available for potential adversaries to exploit;
- Interconnected systems can increase the amount of private information exposed and increase the risk when data is aggregated;
- Increased use of new technologies can introduce new vulnerabilities; and

[4] 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.

[5] 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, Cybersecurity, and Science and Technology, March 24, 2009.

[6] 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.

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

- Expansion of the amount of data that will be collected that can lead to the 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 addition, the Smart Grid will have additional vulnerabilities due not only to its complexity, but also because of its large number of stakeholders and highly time-sensitive operational requirements.

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 and the business processes that support the customer base. 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, in the August 14, 2003, blackout, a contributing factor was issues with communications latency in control systems. With the exception of the initial power equipment problems, the ongoing and cascading failures were primarily due to problems in providing the right information to the right individuals within the right time period. 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.

Development of the *Guidelines for Smart Grid Cyber Security* began with the establishment of a Cyber Security Coordination Task Group (CSCTG) in March 2009 that was established and is led by the National Institute of Standards and Technology (NIST). The CSCTG now numbers more than 475 participants from the private sector (including vendors and service providers), manufacturers, various standards organizations, academia, regulatory organizations, and federal agencies. This group was renamed under the Smart Grid Interoperability Panel (SGIP) as the Cyber Security Working Group (SGIP-CSWG) in January 2010 (hereafter referred to as the CSWG).

Cyber security is being addressed using a thorough process that results in a high-level set of cyber security requirements. As explained more fully later in this chapter, these requirements were developed (or augmented, where standards/guidelines already exist) using a high-level risk assessment process that is defined in the cyber security strategy section of this report. Cyber security requirements are implicitly recognized as critical in all of the priority action plans discussed in the Special Publication (SP), *NIST Framework and Roadmap for Smart Grid Interoperability Standards,* Release 1.0 (NIST SP 1108), which was published in January 2010.[8]

The Framework document describes a high-level reference model for the Smart Grid, identifies 75 existing standards that can be used now to support Smart Grid development, identifies 15 high-priority gaps and harmonization issues (in addition to cyber security) for which new or

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

revised standards and requirements are needed, documents action plans with aggressive timelines by which designated standards-setting organizations (SSOs) are tasked to fill these gaps, and describes the strategy to establish requirements and standards to help ensure Smart Grid cyber security. This Framework document is the first installment in an ongoing standards and harmonization process. Ultimately, this process will deliver the hundreds of communication protocols, standard interfaces, and other widely accepted and adopted technical specifications necessary to build an advanced, secure electric power grid with two-way communication and control capabilities. The NISTIR expands upon the discussion of cyber security included in the Framework document. The NISTIR is a starting point and a foundation. CSWG will continue to provide additional guidance as the Framework document is updated and expanded to address testing and certification, the development of an overall architecture, and as additional standards are identified.

The CSWG has liaisons to other Smart Grid industry groups to support and encourage coordination among the various efforts. The documented liaisons are listed at http://collaborate.nist.gov/twiki-sggrdi/bin/view/SmartGrid/CSWGLiaisonInformation.

This report is a tool for organizations that are researching, designing, developing, and implementing Smart Grid technologies. The cyber security strategy, risk assessment process, and security requirements included in this report should be applied to the entire Smart Grid system.

Cyber security risks must be addressed as organizations implement and maintain their Smart Grid systems. Therefore, this report may be used as a guideline to evaluate the overall cyber risks to a Smart Grid system during the design phase and during system implementation and maintenance. The Smart Grid risk mitigation strategy approach defined by an organization will need to address the constantly evolving cyber risk environment. The goal is to identify and mitigate cyber risk for a Smart Grid system using a risk methodology applied at the organization and system level, including cyber risks for specific components within the system. This methodology in conjunction with the system-level architecture will allow organizations to implement a Smart Grid solution that is secure and meets the reliability requirements of the electric grid.

The information included in this report is guidance for organizations. NIST is not prescribing particular solutions through the guidance contained in this report. Each organization must develop its own detailed cyber security approach (including a risk assessment methodology) for securing the Smart Grid.

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:

> 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 (and privacy) of the information that is transmitted.

The DOE *Energy Sector-Specific Plan*[9] "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 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.

Traditionally, cyber security for Information Technology (IT) focuses on the protection required to ensure the confidentiality, integrity, and availability of the electronic information communication systems. Cyber security needs to be appropriately applied to the combined power system and IT communication system domains to maintain the reliability of the Smart Grid and privacy of consumer information. Cyber security in the Smart Grid must include a balance of both power and cyber system technologies and processes in IT and power system operations and governance. Poorly applied practices from one domain that are applied into another may degrade reliability.

In the power industry, the focus has been on implementation of equipment that could improve power system reliability. Until recently, communications and IT equipment were typically seen as supporting power system reliability. However, these sectors are becoming more critical to the reliability of the power system. In addition, safety and reliability are of paramount importance in electric power systems. Any cyber security measures in these systems must not impede safe, reliable power system operations.

This report provides guidance to organizations that are addressing cyber security for the Smart Grid (e.g., utilities, regulators, equipment manufacturers and vendors, retail service providers, and electricity and financial market traders). This report is based on what is known at the current time about—

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

- The Smart Grid and cyber security;
- Technologies and their use in power systems; and
- Our understanding of the risk environment in which those technologies operate.

This report provides background information on the analysis process used to select and modify the security requirements applicable to the Smart Grid. The process includes both top-down and bottom-up approaches in the selection and modification 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 Advanced Metering Infrastructure (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 report focuses on Smart Grid operations and not on enterprise operations. However, organizations should capitalize on existing enterprise infrastructures, technologies, support and operational aspects when designing, developing and deploying Smart Grid information systems.

1.3 SMART GRID CYBER SECURITY STRATEGY

The overall cyber security strategy used by the CSWG in the development of this document examined both domain-specific and common requirements when developing a risk mitigation approach to ensure interoperability of solutions across different parts of the infrastructure. The cyber security strategy addressed prevention, detection, response, and recovery. This overall strategy is potentially applicable to other complex infrastructures.

Implementation of a cyber security strategy required 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, which 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 assets, vulnerabilities, and threats and specifying impacts to produce an assessment of risk to the Smart Grid and to its domains and subdomains, such as homes and businesses. Because the Smart Grid includes systems from the IT, telecommunications, and electric sectors, the risk assessment process is applied to all three sectors as they interact in the Smart Grid. The information included in this report is guidance for organizations. NIST is not prescribing particular solutions through the guidance contained in this report. Each organization must develop its own detailed cyber security approach (including a risk assessment methodology) for the Smart Grid.

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

- SP 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective*, NIST, April 2008;
- SP 800-30, *Risk Management Guide for Information Technology Systems,* NIST, July 2002;
- 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 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.

The next step in the Smart Grid cyber security strategy was to select and modify (as necessary) the security requirements. The documents used in this step are listed under the description for Task 3. The security requirements and the supporting analyses included in this report may be used by strategists, designers, implementers, and operators of the Smart Grid (e.g., utilities, equipment manufacturers, regulators) as input to their risk assessment process and other tasks in the security lifecycle of the Smart Grid. The information serves as guidance to the various organizations for assessing risk and selecting appropriate security requirements. NIST is not prescribing particular solutions to cyber security issues through the guidance contained in this document.

The cyber security issues that an organization implementing Smart Grid functionality must address are diverse and complicated. This document includes an approach for assessing cyber security issues and selecting and modifying cyber security requirements. Such an approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment, i.e. a system-of-systems. Each organization's implementation of cyber security requirements should evolve as a result of changes in technology and systems, as well as changes in techniques used by adversaries.

The tasks within this cyber security strategy for the Smart Grid were undertaken by participants in the SGIP-CSWG. The remainder of this subsection describes the tasks that have been or will be performed in the implementation of the cyber security strategy. Also included are the deliverables for each task. Because of the time frame within which this report was developed, the

tasks listed on the following pages have been performed 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 that are the responsibility of the CSWG. The tasks are defined following the figure.

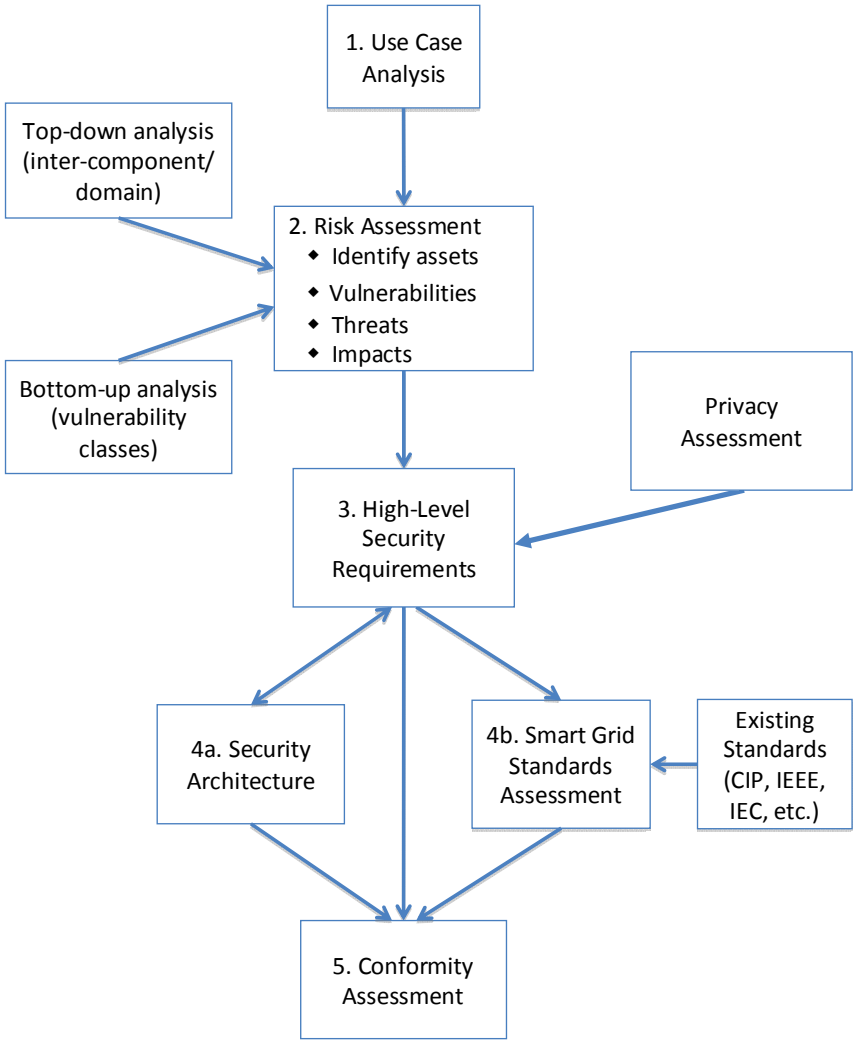

Figure 1-1 Tasks in the Smart Grid Cyber Security Strategy

Task 1. Selection of use cases with cyber security considerations.[10]

The use cases included in Appendix D 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 logical reference model, and selecting and tailoring the security requirements.

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

Task 2. Performance of a risk assessment

The risk assessment, including identifying assets, vulnerabilities, and threats and specifying impacts has been undertaken from a high-level, overall functional perspective. The output was the basis for the selection of security requirements and the identification of gaps in guidance and standards related to the security requirements.

Vulnerability classes: The initial list of vulnerability classes[11] was developed using information from several existing documents and Web sites, e.g., NIST SP 800-82, Common Weakness Enumeration (CWE) vulnerabilities, 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. The vulnerability classes are included in Chapter 6 of this report.

Overall Analysis: Both bottom-up and top-down approaches were used in implementing the risk assessment as specified earlier.

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 security incident. An incident in one infrastructure can potentially cascade to failures in other domains/systems. The bottom-up analysis is included in Chapter 7 of this report.

Top-down analysis: In the top-down approach, logical interface diagrams were developed for the six functional FERC and NIST priority areas that were the focus of the initial draft of this report—Electric Transportation, Electric Storage, Wide Area Situational Awareness, Demand Response, Advanced Metering Infrastructure, and Distribution Grid Management. This report includes a logical reference model for the overall Smart Grid, with logical interfaces identified for the additional grid functionality. Because there are hundreds of interfaces, each logical interface is allocated to one of 22 logical interface categories. Some examples of the logical interface categories are (1) control systems with high data accuracy and high availability, as well as media and computer constraints; (2) business-to-business (B2B) connections; (3) interfaces between sensor networks and controls systems; and (4) interface to the customer site. A set of attributes (e.g., wireless media, inter-organizational interactions, 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.[12] This assessment was done for each logical interface category. The output from this process was used in the selection of security requirements (Task 3).

As with any assessment, a realistic analysis of the inadvertent errors, acts of nature, and malicious threats and their applicability to subsequent risk-mitigation strategies is critical to the overall outcome. The Smart Grid is no different. It is recommended that all organizations take a

[11] 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.

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

realistic view of the hazards and 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. The following table summarizes the categories of adversaries to information systems. These adversaries need to be considered when performing a risk assessment of a Smart Grid information system.

Table 1-1 Categories of Adversaries to Information Systems

Adversary	Description
Nation States	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, which is normally not well organized or financed. Normally consists of few individuals, or of one individual acting alone.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
Disgruntled Employees	Angry, dissatisfied individuals with the potential to inflict harm on the Smart Grid network or related systems. This can represent an insider threat depending on the current state of the individual's employment and access to the systems.
Careless or Poorly Trained Employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to Smart Grid systems. This is another example of an insider threat or adversary.

Task 3. Specification of high-level security requirements.

For the assessment of specific security requirements and the selection of appropriate security technologies and methodologies, both cyber security experts and power system experts were needed. The cyber security experts brought a broad awareness of IT and control system security technologies, while the power system experts brought a deep understanding of traditional power system methodologies for maintaining power system reliability.

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 CSWG used three source documents for the cyber security requirements in this report[13]—

[13] NIST SP 800-53 is mandatory for federal agencies, and the NERC CIPs are mandatory for the Bulk Power System. This report is a guidance document and is not a mandatory standard.

- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009;
- NERC CIP 002, 003-009, version 3; and
- *Catalog of Control Systems Security: Recommendations for Standards Developers*, Department of Homeland Security, March 2010.

These security requirements were then modified for the Smart Grid. To assist in assessing and selecting the requirements, a cross-reference matrix was developed. This matrix, Appendix B, maps the Smart Grid security requirements in this report to the security requirements in SP 800-53, The DHS Catalog, and the NERC CIPs. Each requirement falls in one of three categories: governance, risk and compliance (GRC); common technical; and unique technical. The GRC requirements are applicable to all Smart Grid information systems within an organization and are typically implemented at the organization level and augmented, as required, for specific Smart Grid information systems. The common technical requirements are applicable to all Smart Grid information systems within an organization. The unique technical requirements are allocated to one or more of the logical interface categories defined in the logical reference model included in Chapter 2. Each organization must determine the logical interface categories that are included in each Smart Grid information system. These requirements are provided as guidance and are not mandatory. Each organization will need to perform a risk assessment to determine the applicability of the requirements to their specific situations.

Organizations may find it necessary to identify alternative, but compensating security requirements. A compensating security requirement is implemented by an organization in lieu of a recommended security requirement to provide a 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 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, existing power system capabilities may be used to meet specific security requirements.

Coordination with the Advanced Security Acceleration Project for the Smart Grid: The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) has made significant contributions to the subgroups that developed this report. ASAP-SG is a utility-driven, public-private collaborative between DOE, the Electric Power Research Institute (EPRI), and a large group of leading North American utilities to develop system-level security requirements for smart grid applications such as advanced metering, third-party access for customer usage data, distribution automation, home area networks, synchrophasors, etc. ASAP-SG is capturing these requirements in a series of Security Profiles, which are submitted to the SG Security Working Group within the UCA International Users Group (UCAIug) for ratification and to the CSWG as input for this report. The collaboration between the CSWG and ASAP-SG has proven most beneficial, as this report provides context and establishes high-level logical interfaces for the ASAP-SG Security Profiles while the Security Profiles provide detailed, actionable, and tailored controls for those building and implementing specific Smart Grid systems.

To date, ASAP-SG has produced two Security Profiles and is nearing completion on a third. The Security Profile for Advanced Metering Infrastructure ("AMI Security Profile") has been ratified

by the AMI-SEC Task Force within the UCAIug and provides prescriptive, actionable guidance for how to build-in and implement security from the meter data management system up to and including the home area network interface of the smart meter. The AMI Security Profile served as the basis for early discussions of security for advanced metering functions, eventually informing selection of requirements for the Logical Interface Categories 13 and 14.

The Security Profile for Third Party Data Access ("3PDA Security Profile") is currently under review by a Usability Analysis team within the UCAIug SG Security Working Group, and delineates the security requirements for individuals, utilities, and vendors participating in three-way relationships that involve the ownership and handling of sensitive data (e.g., electric utility customers who want to allow value added service providers to access electric usage data that is in the custody of the customer's utility). The 3PDA Security Profile served as a reference point for many discussions on the subject of privacy, and informed several aspects of Chapter Five – Privacy and the Smart Grid.

Upon completion, the Security Profile for Distribution Management ("DM Security Profile") will address automated distribution management functions including steady state operations and optimization. For this profile "distribution automation" is treated as a specific portion of distribution management related to automated system reconfiguration and SCADA, and is within scope. Publicly available versions of ASAP-SG documentation may be found on SmartGridiPedia at http://www.smartgridipedia.org.

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 privacy recommendations provide a set of privacy requirements that should be considered when organizations implement Smart Grid information systems. These privacy requirements augment the security requirements specified in Chapter 3.

Task 4a. Development of a logical reference model.

Using the conceptual model included in this report, the FERC and NIST priority area use case diagrams, and the additional areas of AMI and distribution grid management, the CSWG developed a more granular logical reference model for the Smart Grid. This logical reference model consolidates the individual diagrams into a single diagram and expands upon the conceptual model. The additional functionality of the Smart Grid that is not included in the six use case diagrams is included in this logical reference model. The logical reference model identifies logical communication interfaces between actors. This logical reference model is included in Chapter 2 of this report. Because this is a high-level logical reference model, there may be multiple implementations of the logical reference model. In the future, the NIST conceptual model and the logical reference model included in this report will be used by the SGIP Architecture Committee (SGAC) to develop a single Smart Grid architecture. Subsequently, this Smart Grid architecture will be used by the CSWG to revise the logical security architecture included in this report.

Task 4b. Assessment of Smart Grid standards.

In Task 4b, standards that have been identified as potentially relevant to the Smart Grid by the Priority Action Plan (PAP) teams and the SGIP will be assessed to determine relevancy to Smart Grid security. In this process, gaps in security requirements will be identified and

recommendations will be made for addressing these gaps. Also, conflicting standards and standards with security requirements not consistent with the security requirements included in this report will be identified with recommendations. This task is ongoing, and the results will be published in a separate document.

Task 5. Conformity Assessment.

The final task is to develop a conformity assessment program for security. This program will be coordinated with the activities defined by the testing and certification standing committee of the SGIP.

1.4 OUTSTANDING ISSUES AND REMAINING TASKS

The following areas need to be addressed in follow-on CSWG activities.

1.4.1 Additional Cyber Security Strategy Areas

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 of the current power grid (e.g., power outages caused by squirrels). Mitigating physical-only attacks is beyond the scope of this report, 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.

1.4.2 Future Research and Development (R&D) Topics

There are some R&D themes that are partially addressed in this document that warrant further discussion. There are other R&D themes that are relatively new. The following list consists of topics the R&D group plans to address in the future:

- Synchrophasor Security / NASPInet;
- Anonymization;
- Use of IPv6 in large scale real time control systems;
- Behavioral Economics/Privacy;
- Cross-Domain security involving IT, Power, and Transportation systems; and
- Remote Disablement/Switch of Energy Sources.

1.4.3 Future Cryptography and Key Management Areas

Some topics that will be further developed in the future include:

- Smart Grid adapted PKI: exploration of how to adapt PKI systems for the grid and its various operational and device/system requirements.
- Secure and trusted device profiles: development of a roadmap of different levels of hardware based security functionality that is appropriate for various types of Smart Grid devices.

- Applicable standards: identification and discussion of existing standards that can be used or adapted to meet the cryptography and key management requirements or solve the problems that have been identified.
- Certificate Lifetime: future work should be done to ensure that appropriate guidelines and best practices are established for the Smart Grid community.

1.4.4 Future Privacy Areas

There are privacy concerns for individuals within business premises, such as hotels, hospitals, and office buildings, in addition to privacy concerns for transmitting Smart Grid data across country borders. The privacy use cases included in this report do not address business locations or cross border data transmission. These are topics identified for further investigation.

1.4.5 Roadmap for Vulnerability Classes

The content of the vulnerability chapter is being used across a wide spectrum of industry, from procurement processes in utilities to SDOs and manufacturers, because of the focus on specific and technical analysis that can be responded to with concrete and actionable solutions. This is an encouraging direction for the entire industry. Therefore, we want to encourage the direction of our material becoming more usable across the range of industry. To meet this goal, listed below are some high-level points that will form our roadmap for future activities—

- **Design considerations:** There will be a continued expansion of this material to cover more bottom-up problems and industry issues to provide information that can more directly inform technical elements of procurement processes, as well as specifications and solutions for standards and product development.
- **Specific topics:** Some bottom-up problems and design considerations that began development but were not at a sufficient enough level for inclusion in this version include—
  - Authenticity and trust in the supply chain, and
  - Vulnerability management and traceability in the supply chain.

  The first issue above was driven by the fact that there have been real instances in the broader market with devices that had unauthentic parts or were themselves totally unauthentic. The motives thus far behind these deceptions appeared to be criminal for the sake of economic gain in selling lower cost and quality hardware under the banner of a higher cost and quality brand. This has led to unanticipated failures in the field. This situation brings a strong possibility of reliability issues to the Smart Grid, and if the direction of this threat becomes more malicious with the intent to insert back doors or known flawed components subject to exploitable vulnerability it will elevate the situation to a new level of possible impact.

  Vulnerability management in the supply chain will be focused on the fact that systems and individual devices have become a disparate collection of software and hardware components across very complex supply chains. As a result, it may not be clear to asset owners or the manufacturers directly supplying them the extent to which they may be affected by many reported vulnerabilities in underlying, unknown, and embedded components.

CHAPTER TWO
LOGICAL ARCHITECTURE AND INTERFACES OF THE SMART GRID

This chapter includes a logical reference model 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. In the future, the NIST conceptual model and the logical reference model included in this report will be used by the SGIP Architecture Committee (SGAC) to develop a single Smart Grid architecture that will be used by the CSWG to revise the logical security architecture included in this report. Figure 2-3 presents the logical reference model 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 subdomains. 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 in this case are representative examples and do not encompass 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. Table 2-1 complements the logical reference model diagram (Figure 2-3) with a description of the actors associated with the logical reference model.

The logical reference model represents a blending of the initial set of use cases, requirements that were developed at the NIST Smart Grid workshops, the initial NIST Smart Grid Interoperability Roadmap, and the logical interface diagrams for the six FERC and NIST priority areas: electric transportation, electric storage, advanced metering infrastructure (AMI), wide area situational awareness (WASA), distribution grid management, and customer premises.[14] These six priority areas are depicted in individual diagrams with their associated tables. These lower-level diagrams were originally produced at the NIST Smart Grid workshops and then revised for this report. They provide a more granular view of the Smart Grid functional areas. These diagrams are included in Appendix F.

All of the logical interfaces included in the six diagrams are included in the logical reference model. The format for the reference number for each logical interface is UXX, where U stands for universal and XX is the interface number. The reference number is the same on the individual application area diagrams and the logical reference model. This logical reference model focuses on a short-term view (1–3 years) of the proposed Smart Grid and is only a sample representation.

The logical reference model 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 illustrates, at a high level, the diversity of systems as well as a first representation of associations between

[14] This was previously named Demand Response.

systems and components of the Smart Grid. The list of actors is a subset of the full list of actors for the Smart Grid and is not intended to be a comprehensive list. This logical reference model is a high-level logical architecture and does not imply any specific implementation.

2.1 THE SEVEN DOMAINS TO THE LOGICAL REFERENCE MODEL

The *NIST Framework and Roadmap* document identifies seven domains within the Smart Grid: Transmission, Distribution, Operations, Bulk Generation, Markets, Customer, and Service Provider. 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. The various actors are needed to transmit, store, edit, and process the information needed within the Smart Grid. To enable Smart Grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 2-1.

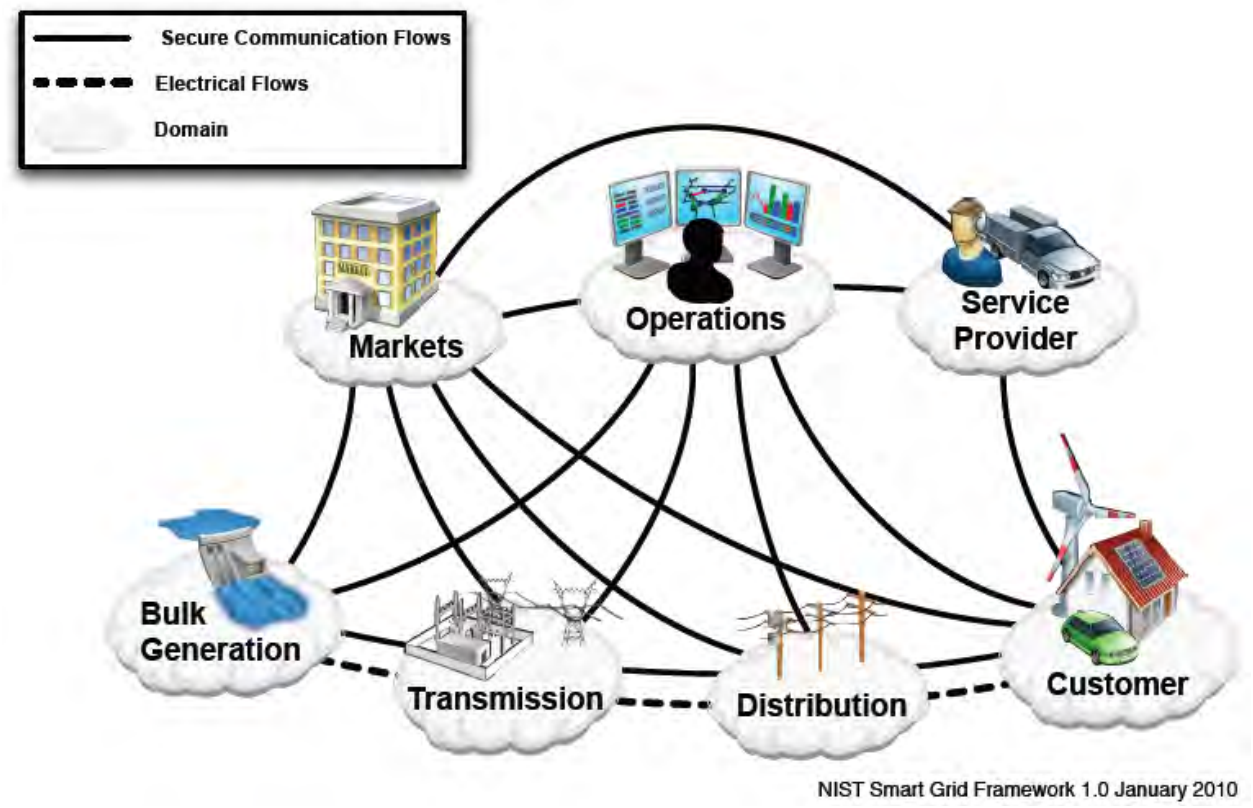

Figure 2-1 Interaction of Actors in Different Smart Grid Domains through Secure Communication Flows

The diagram below (Figure 2-2) expands upon this figure and depicts a composite high-level view of the actors within each of the Smart Grid domains. This high-level diagram is provided as a reference diagram. Actors are devices, systems, or programs that make decisions and exchange information necessary for executing applications within the Smart Grid. The diagrams included later in this chapter expand upon this high-level diagram and include logical interfaces between actors and domains.

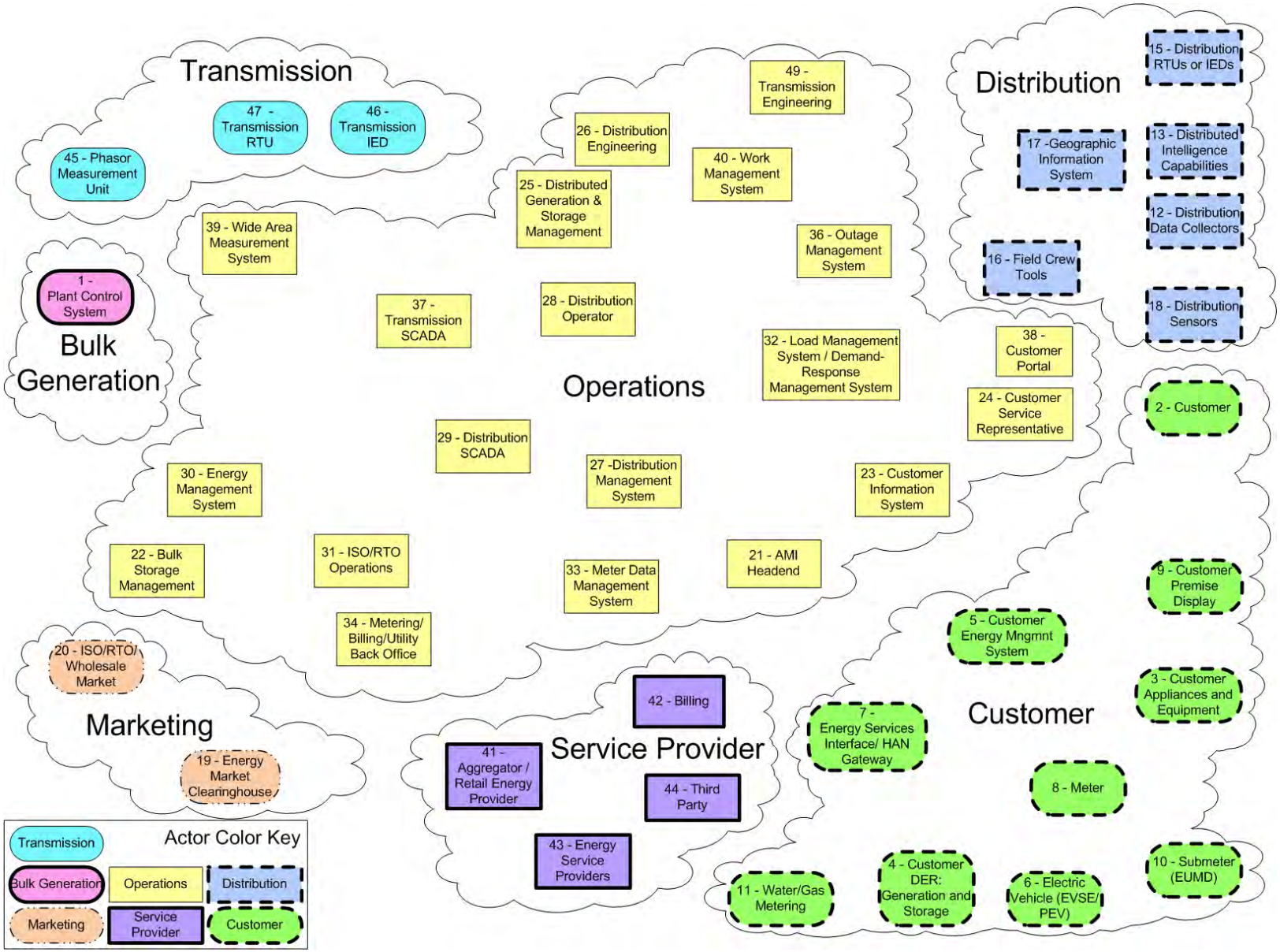

Figure 2-2 Composite High-level View of the Actors within Each of the Smart Grid Domains

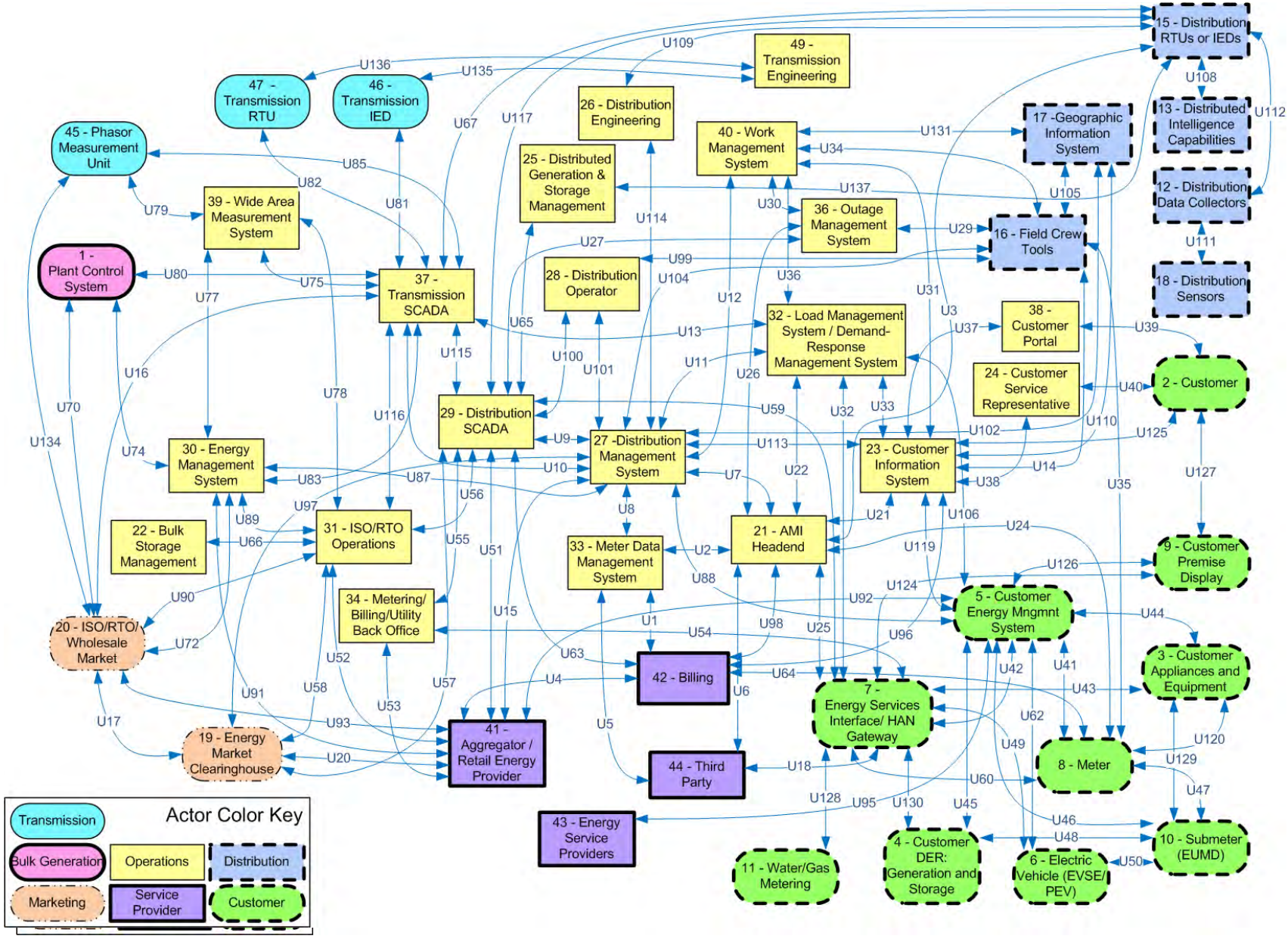

Figure 2-3 Logical Reference Model

Table 2-1 Actor Descriptions for the Logical Reference Model

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 or device that communicates with devices in the home. The application service or device may have interfaces to the meter to read usage data 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 third party-offered service, a consumer-specified policy, a consumer-owned device, or a manual control by the utility or consumer.
6	Customer	Electric Vehicle Service Element/Plug-in Electric Vehicle	EVSE/PEV	A vehicle driven primarily 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	Home Area Network Gateway	HAN Gateway	An interface between the distribution, operations, service provider, and customer domains and the devices within the customer domain.
8	Customer	Meter		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		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 collecting data from multiple sources and modifying/transforming it into different form factors.
13	Distribution	Distributed Intelligence Capabilities		Advanced automated/intelligence application that operates in a normally autonomous mode from the centralized control system to increase reliability and responsiveness.
14	Distribution	Distribution Automation Field Devices		Multifeatured 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 handheld 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.

Actor Number	Domain	Actor	Acronym	Description
19	Marketing	Energy Market Clearinghouse		Widearea 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 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 operate the market. From the Electric Power Supply Association (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."[15]
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 Meter Data Management System (MDMS) and the AMI network.[16]
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]).

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

[16] Headend (head end)—A central control device required by some networks (e.g., LANs or MANs) to provide such centralized functions as remodulation, retiming, message accountability, contention control, diagnostic control, and access to a gateway. See http://en.wikipedia.org/wiki/Head_end.

Actor Number	Domain	Actor	Acronym	Description
25	Operations	Distributed Generation and Storage Management		Distributed generation is also referred to as on-site generation, dispersed generation, embedded generation, decentralized generation, decentralized energy, or distributed energy. This process generates electricity from many small energy sources for use or storage on dispersed, small devices or systems. This approach reduces the amount of energy lost in transmitting electricity because the electricity is generated very near where it is used, perhaps even in the same building. [17]
26	Operations	Distribution Engineering		A technical function of planning or managing the design or upgrade 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, online 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 system.
29	Operations	Distribution Supervisory Control and Data Acquisition	SCADA	A type of control system that transmits individual device status, manages energy consumption by controlling compliant devices, and allows operators to directly control power system equipment.

[17] Description summarized from http://en.wikipedia.org/wiki/Distributed_generation.

Actor Number	Domain	Actor	Acronym	Description
30	Operations	Energy Management System	EMS	A system of computer-aided tools used by operators of electric utility grids to monitor, controls, 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		Widearea power system control center providinghigh-level load management and security analysis for the transmission grid, typically using an EMS with generation applications and network analysis applications.
32	Operations	Load Management Systems/Demand Response Management System	LMS/DRMS	An LMS issues load management commands to appliances or 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 preprogrammed 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 may also be referred to as a 'billing meter.'

Actor Number	Domain	Actor	Acronym	Description
34	Operations	Metering/Billing/Utility Back Office		Back office utility systems for metering and billing.
36[18]	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 location 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. • Estimation of restoration time. • 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 allowing operators to directly control power system equipment.
38	Operations	Customer Portal		A computer or service that makes available Web pages. Typical services may include: customer viewing of their energy and cost information online, enrollment in prepayment electric services, and enablement of third-party monitoring and control of customer equipment.
39	Operations	Wide Area Measurement System	WAMS	Communication system that monitors all phase measurements and substation equipment over a large geographical base that can use visual modeling and other techniques to provide system information to power system operators.

[18] Actor 35 was deleted during development. Actors will be renumbered in the next version of this document.

Actor Number	Domain	Actor	Acronym	Description
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/Retail Energy Provider		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 obtain reimbursement from the customer.
43	Service Provider	Energy Service Provider	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 business function outside of the utility.
45	Transmission	Phasor Measurement Unit	PMU	Measures the electrical parameters of an electricity grid with respect to universal time (UTC) such as phase angle, amplitude, and frequency to determine the state 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.
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.
48[19]	Operations	Security/Network/System Management		Security/Network/System management devices that monitor and configure the security, network, and system devices.
49	Transmission	Transmission Engineering		Equipment designed for more than 345,000 volts between conductors.

[19] Actor 48 is included in logical interface category 22 for security. It is not included in the logical reference model.

2.2 LOGICAL SECURITY ARCHITECTURE OVERVIEW

Smart Grid technologies will introduce millions of new components to the electric grid. Many of these components are critical to interoperability and reliability, will communicate bidirectionally, and will be tasked with maintaining confidentiality, integrity, and availability (CIA) vital to power systems operation.

The definitions of CIA are defined in statue and can be summarized as follows:

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.

The high-level security requirements address the goals of the Smart Grid. They describe ***what*** the Smart Grid needs to deliver to enhance security. The logical security architecture describes ***where***, at a high level, the Smart Grid will provide security.

This report has identified cyber security requirements for the different logical interface categories. Included in Appendix B are categories of cyber security technologies and services that are applicable to the common technical security requirements. This list of technologies and services is not intended to be prescriptive; rather, it is to be used as guidance.

2.2.1 Logical Security Architecture Key Concepts and Assumptions

A Smart Grid's logical security architecture is constantly in flux because threats and technology evolve. The architecture subgroup specified the following key concepts and assumptions that were the foundation for the logical security architecture.

- **Defense-in-depth strategy:** Security should be 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 information (including customer), assets, power systems, and communications and IT infrastructures through layered defenses (e.g., firewalls, intrusion detection systems, antivirus 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.
- **Power system availability:** Power system resiliency to events potentially leading to outages has been the primary focus of power system engineering and operations for

decades. Existing power system design and capabilities have been successful in providing this availability for protection against inadvertent actions and natural disasters. These existing power system capabilities may be used to address the cyber security requirements.

The logical security architecture seeks to mitigate threats and threat agents from exploiting system weaknesses and vulnerabilities that can impact the operating environment. A logical security architecture needs to provide protections for data at all interfaces within and among all Smart Grid domains. The logical security architecture baseline assumptions are as follows:

1. A logical security architecture promotes an iterative process for revising the architecture to address new threats, vulnerabilities, and technologies.
2. All Smart Grid systems will be targets.
3. There is a need to balance the impact of a security breach and the resources required to implement mitigating security measures. (Note: The assessment of cost of implementing security is outside the scope of this report. However, this is a critical task for organizations as they develop their cyber security strategy, perform a risk assessment, select security requirements, and assess the effectiveness of those security requirements.)
4. The logical security architecture should be viewed as a business enabler for the Smart Grid to achieve its operational mission (e.g., avoid rendering mission-purposed feature sets inoperative).
5. The logical security architecture is not a one-size-fits-all prescription, but rather a framework of functionality that offers multiple implementation choices for diverse application security requirements within all electric sector organizations.

2.3 LOGICAL INTERFACE CATEGORIES

Each logical interface in the logical reference model 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 (included in Appendix G) can be used as guidelines by organizations that are developing a cyber security strategy and implementing a risk assessment to select security requirements. This information may also be used by vendors and integrators as they design, develop, implement, and maintain the security requirements. Included below are a listing of all of the logical interfaces by category, the descriptions of each logical interface category, and the associated security architecture diagram. Examples included in the discussions below are not intended to be comprehensive. The user should assess the existing and proposed Smart Grid information system as part of determining which logical interface category should include a specific interface. Listed in each diagram are the unique technical requirements. These security requirements are included in the next chapter.

Table 2-2 Logical Interfaces by Category

Logical Interface Category	Logical Interfaces
1. 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, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
2. 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	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
4. 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	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
5. 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, U65, U66, U89
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U7, U10, U13, U16, U56, U74, U80, U83, U87, U115, U116
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U22, U26, U31, U63, U96, U98, U110

Logical Interface Category	Logical Interfaces
8. 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, U55
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U4, U17, U20, U51, U52, U53, U57, U58, U70, U72, U90, U93, U97
10. 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, U59, U75, U91, U106, U113, U114, U131
11. 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
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	U108, U112
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U8, U21, U25, U32, U95, U119, U130
14. 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	U8, U21, U25, U32, U95, U119, U130
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U42, U43, U44, U45, U49, U62, U120, U124, U126, U127

Logical Interface Category	Logical Interfaces
16. 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, U37, U38, U39, U40, U88, U92, U100, U101, U125
17. 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, U99, U104, U105
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41, U46, U47, U48, U50, U54, U60, U64, U128, U129
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	U77, U78, U134
20. 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, U109
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	U5
22. 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	U133 (includes interfaces to actors 17-Geographic Information System, 12 – Distribution Data Collector, 38 – Customer Portal, 24 – Customer Service Representative, 23 – Customer Information System, 21 – AMI Headend, 42 – Billing, 44 – Third Party, 43 – Energy Service Provider, 41 – Aggregator / Retail Energy Provider, 19 – Energy Market Clearinghouse, 34 – Metering / Billing / Utility Back Office)

2.3.1 Logical Interface Categories 1—4

Logical Interface Category 1: Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints

Logical Interface Category 2: Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints

Logical Interface Category 3: Interface between control systems and equipment with high availability, without compute or bandwidth constraints

Logical Interface Category 4: Interface between control systems and equipment without high availability, without compute or bandwidth constraints

Logical interface categories 1 through 4 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 or without high availability. The interface communication channel is categorized with or without computational and/or bandwidth constraints. All activities involved with logical interface categories 1 through 4 are typically machine-to-machine actions. Furthermore, communication modes and types are similar between logical interface categories 1 through 4 and are defined as follows:

- Interface Data Communication Mode
  - Near Real-Time Frequency Monitoring Mode (ms, subcycle based on a 60 Hz system) (may or may not include control action communication)
  - High Frequency Monitoring Mode (2 s ≤ 60 s scan rates)
  - Low Frequency Monitoring Mode (scan/update rates in excess of 1 min, 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 that vary between and distinguish each logical interface category are the availability requirements for the interface and the computational/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 because it is supporting critical monitoring and switching functions or a MODERATE to LOW availability if supporting an asset-monitoring application.

- Communications and Computational Constraints –- Computational constraints are associated with cryptography requirements on the interface. The use of cryptography typically has high CPU needs for mathematical calculations, although it is feasible to implement cryptographic processing in peripheral hardware. Existing devices like RTUs, substation IEDs, meters, and others are typically not equipped with sufficient digital hardware to perform cryptography 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 1 through 4 can be defined as follows:

1. Interface between control systems and equipment with high availability and with computational 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 automatic generation control (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; and
    - Between transmission SCADA in support of contingency analysis and substation equipment for monitoring data using high frequency mode.
2. Interface between control systems and equipment without high availability and with computational 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; and
    - 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.
3. Interface between control systems and equipment with high availability without computational 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; and
- Between IEDs (peer-to-peer) for power system protection, including transfer trip signals between equipment in different substations.

4. Interface between control systems and equipment without high availability, without computational and/or bandwidth constraints:
   - Between field device and asset monitoring system for monitoring data using a low frequency mode;
   - Between field devices (relays, digital fault recorders [DFRs], power quality [PQ]) and event analysis systems for event, disturbance, and PQ 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; and
   - 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.

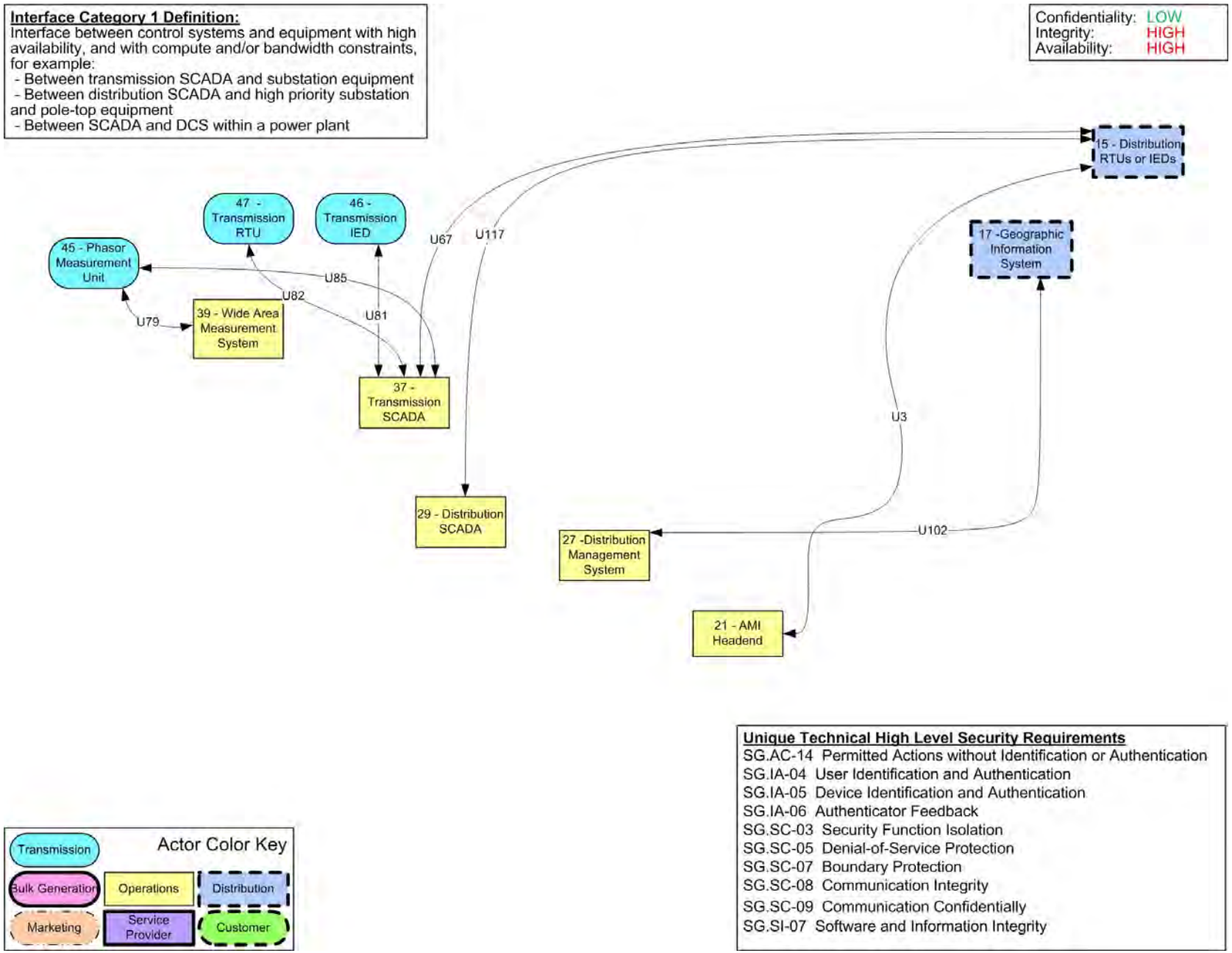

Figure 2-4 Logical Interface Category 1

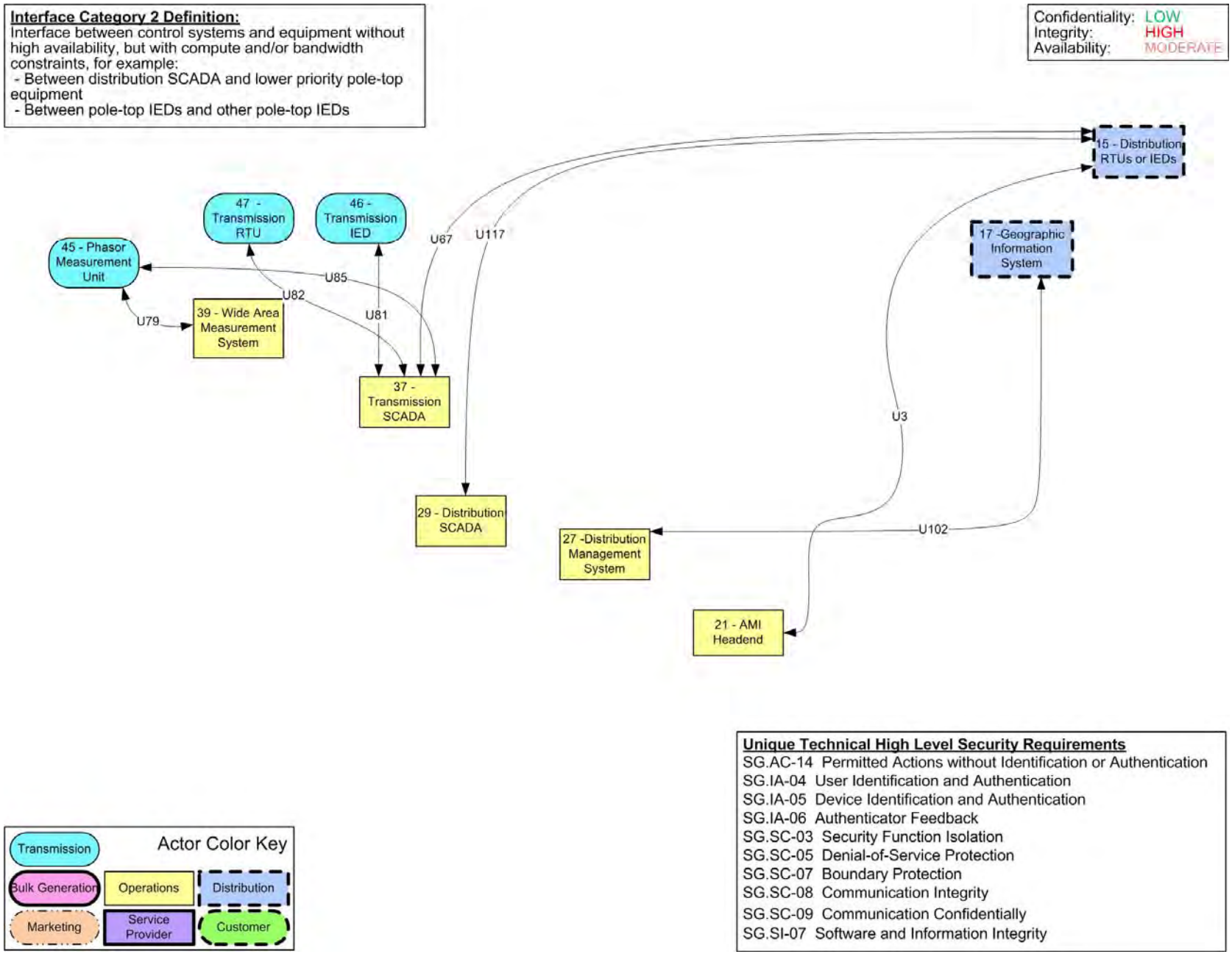

Figure 2-5 Logical Interface Category 2

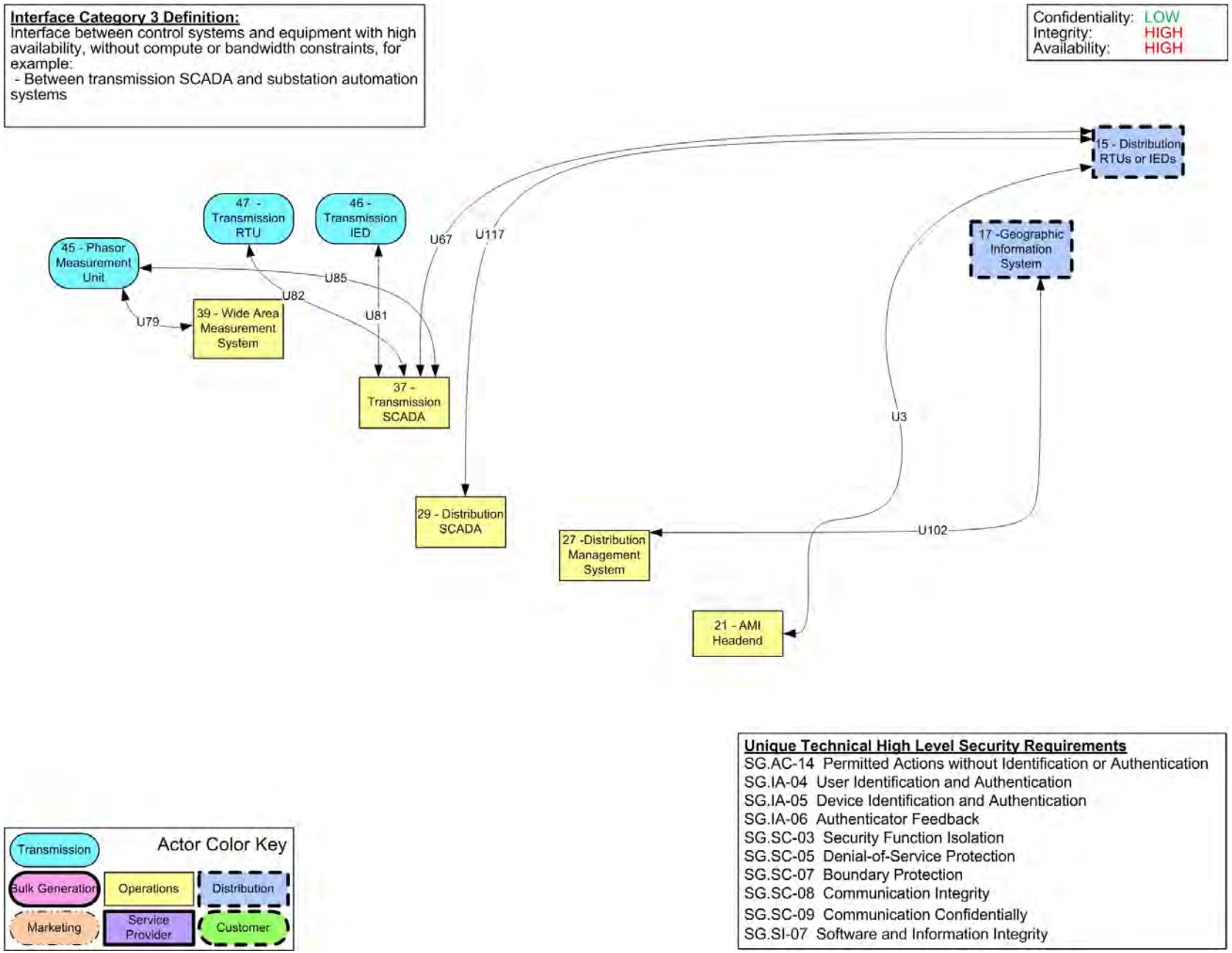

Figure 2-6 Logical Interface Category 3

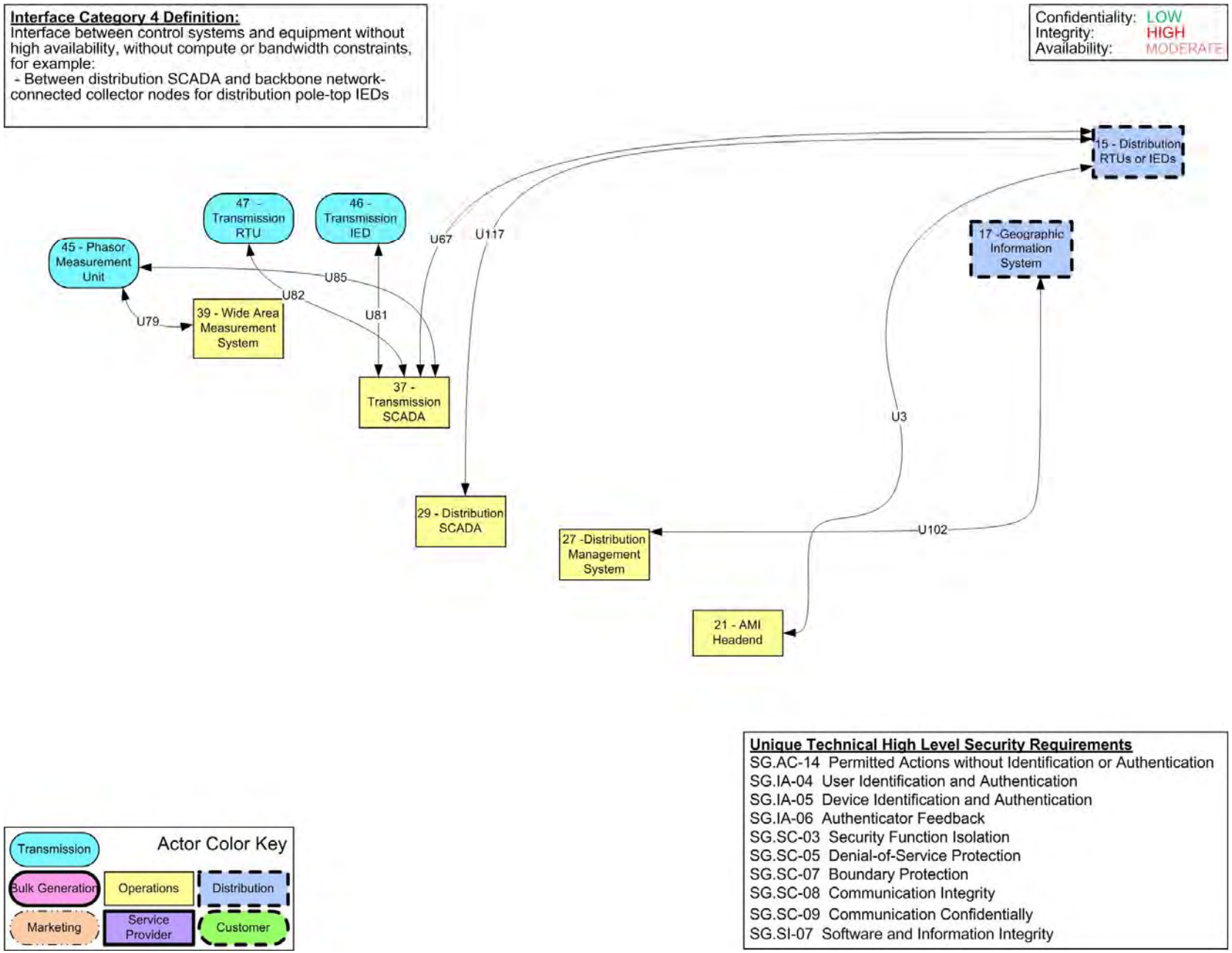

Figure 2-7 Logical Interface Category 4

2.3.2 Logical Interface Category 5: Interface between control systems within the same organization

Logical interface category 5 covers the interfaces between control systems within the same organization, for example:

- Between multiple data management 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 (wide area networks [WANs] and/or local area networks [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.

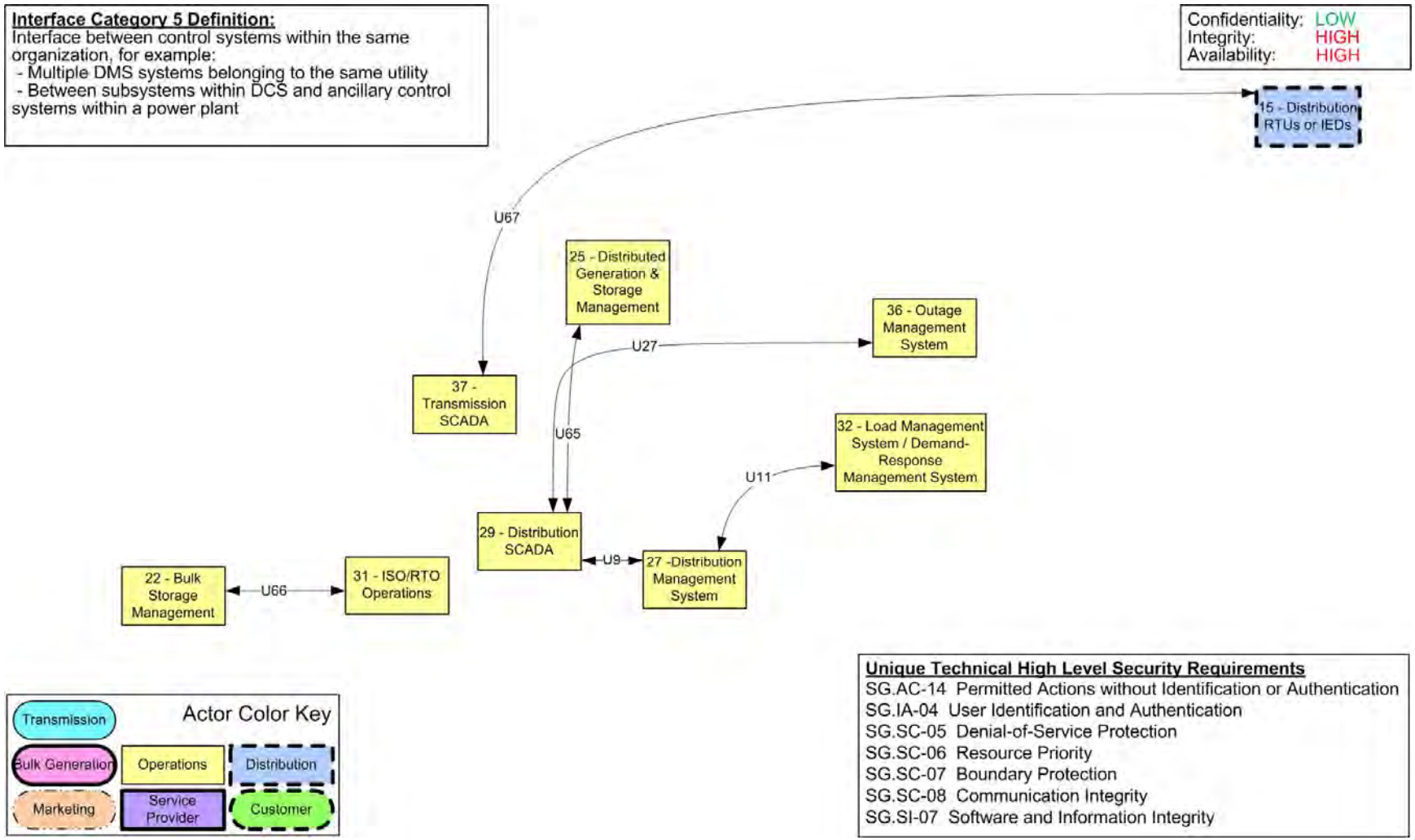

Figure 2-8 Logical Interface Category 5

2.3.3 Logical Interface Category 6: Interface between control systems in different organizations

Logical interface category 6 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; and
- 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.
- Since the control systems are in different organizations, the establishment and maintenance of the chain of trust is more important.

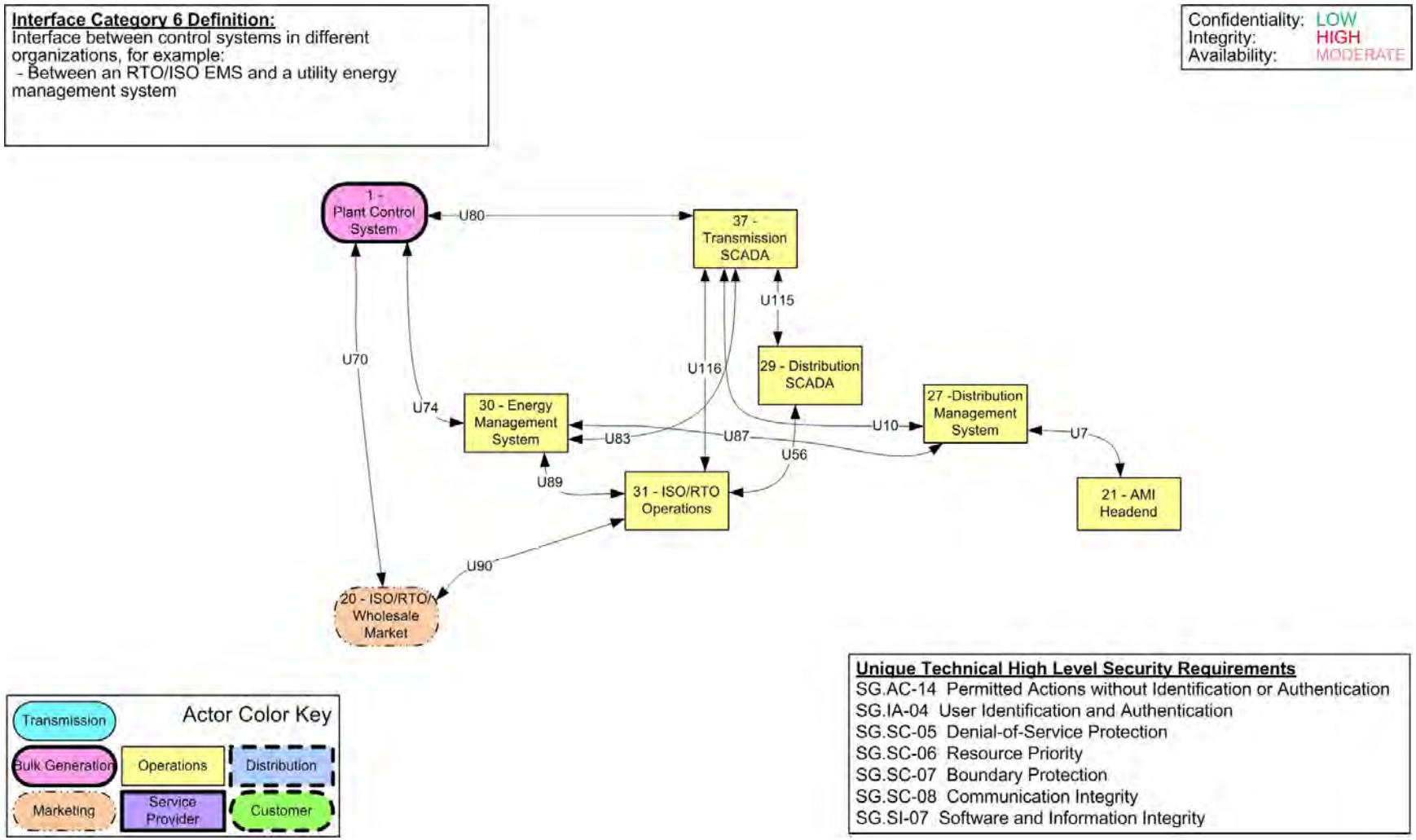

Figure 2-9 Logical Interface Category 6

2.3.4 Logical Interface Categories 7—8

Logical Interface Category 7: Interface between back office systems under common management authority

Logical Interface Category 8: Interface between back office systems not under common management authority

Logical interface category 7 covers the interfaces between back office systems that are under common management authority, e.g., between a CIS and a MDMS. Logical interface category 8 covers the interfaces between back office systems that are not under common management authority, e.g., between a third-party billing system and a utility MDMS. These logical interface categories are focused on confidentiality and privacy rather than on power system reliability.

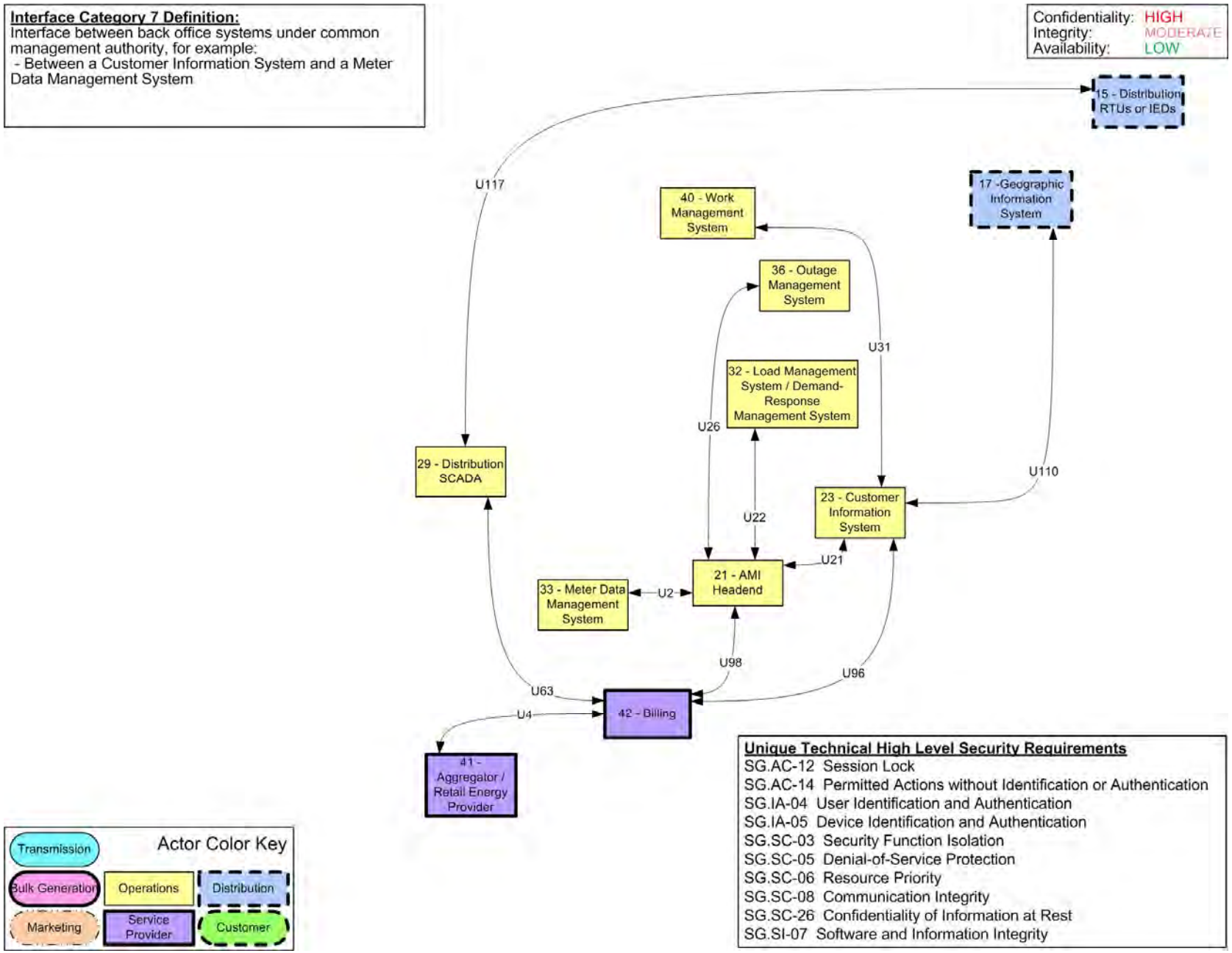

Figure 2-10 Logical Interface Category 7

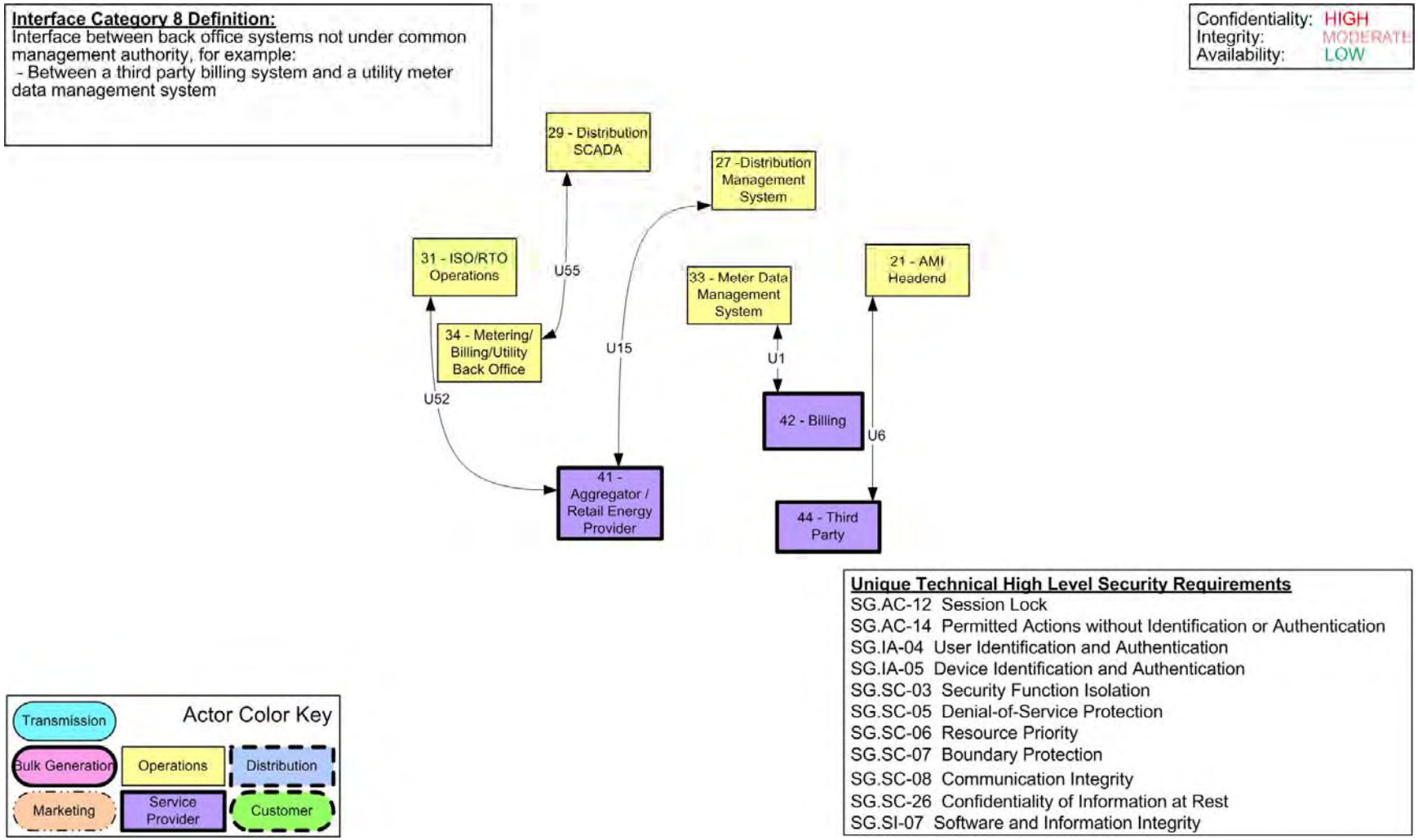

Figure 2-11 Logical Interface Category 8

2.3.5 Logical Interface Category 9: Interface with business to business (B2B) connections between systems usually involving financial or market transactions

Logical interface category 9 covers the interface with 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 needs to be considered 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 maintaining 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 inadvertently 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 that growth will occur.
- However, systems and procedures for market interactions are very mature industry concepts. The primary requirement, therefore, is to utilize those concepts and protections in the newly emerging retail energy market.

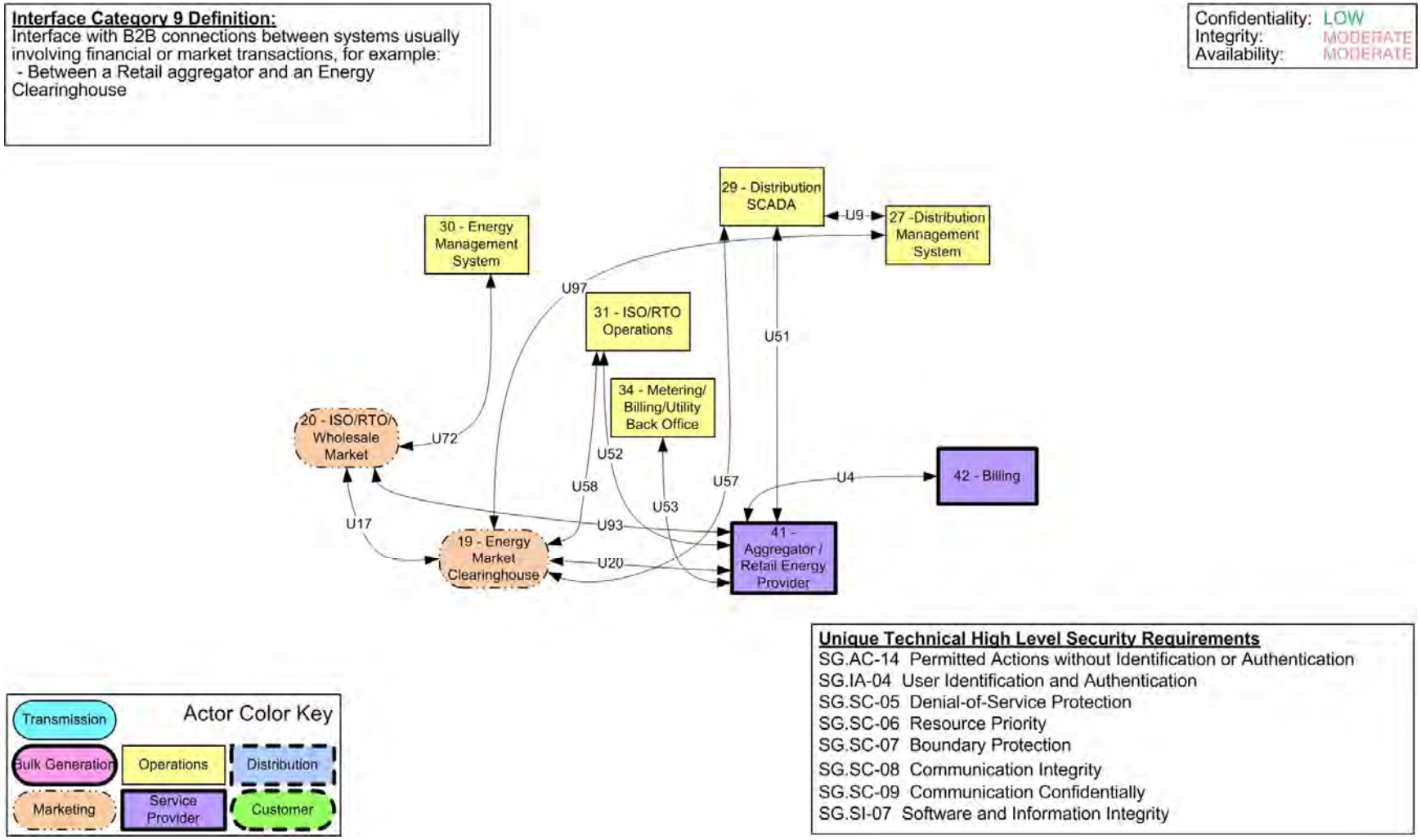

Figure 2-12 Logical Interface Category 9

2.3.6 Logical Interface Category 10: Interface between control systems and non-control/ corporate systems

Logical interface category 10 covers the interfaces between control systems and non-control/corporate systems, for example:

- Between a WMS and a GIS;
- Between a DMS and a CIS;
- Between an OMS and the AMI headend system; and
- Between an OMS and a WMS.

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 International Electrotechnical Commission (IEC) Common Information Model (CIM)[20] and the National Rural Electric Cooperative Association (NRECA) MultiSpeak® specification expected to become the most common standards, although other efforts for special interfaces (e.g., GIS) are also under way.

[20] IEC 61970/69 Common Information Model.

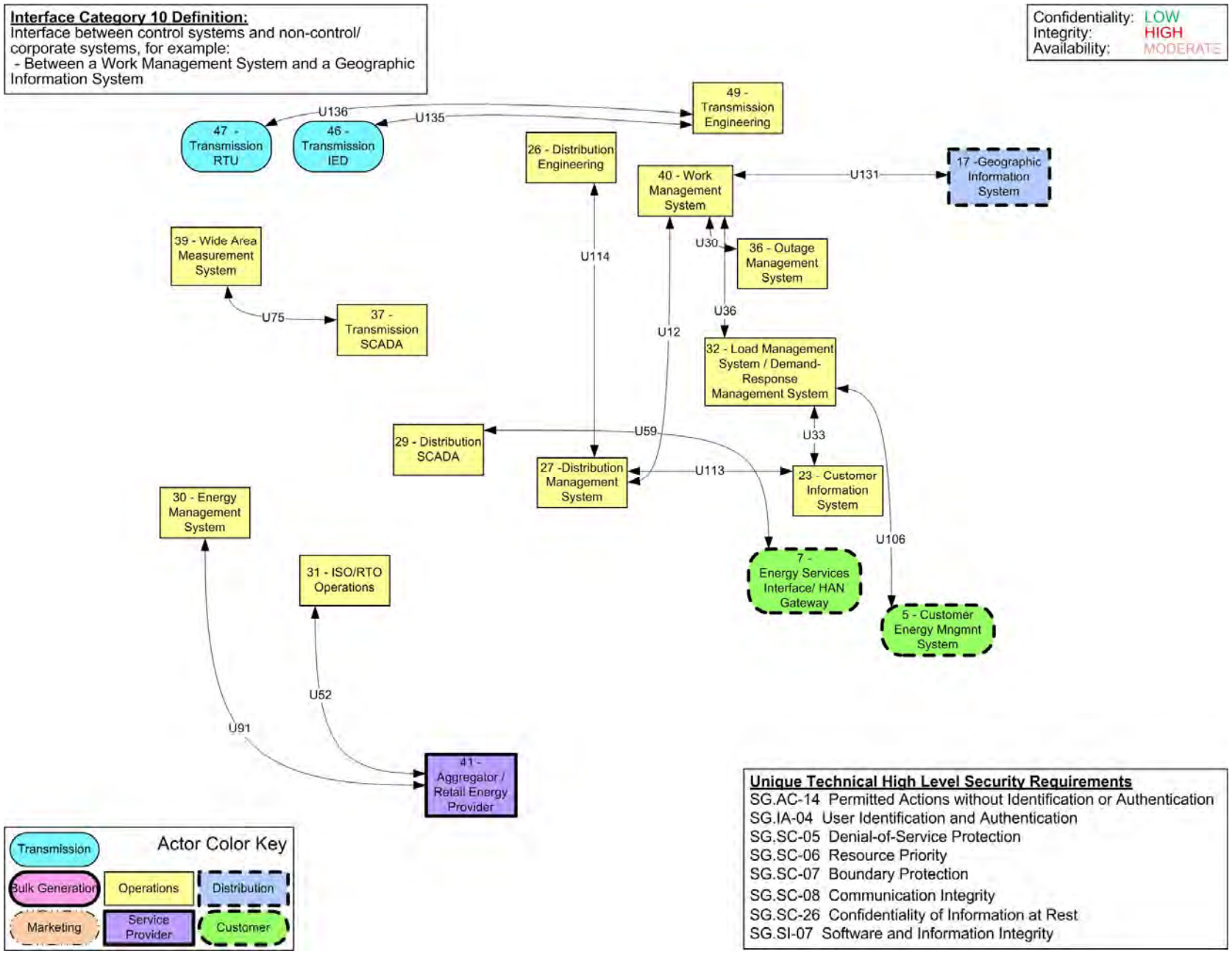

Figure 2-13 Logical Interface Category 10

2.3.7 Logical Interface Category 11: Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements

Logical interface category 11 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 computational capability and often limited in communication bandwidth.

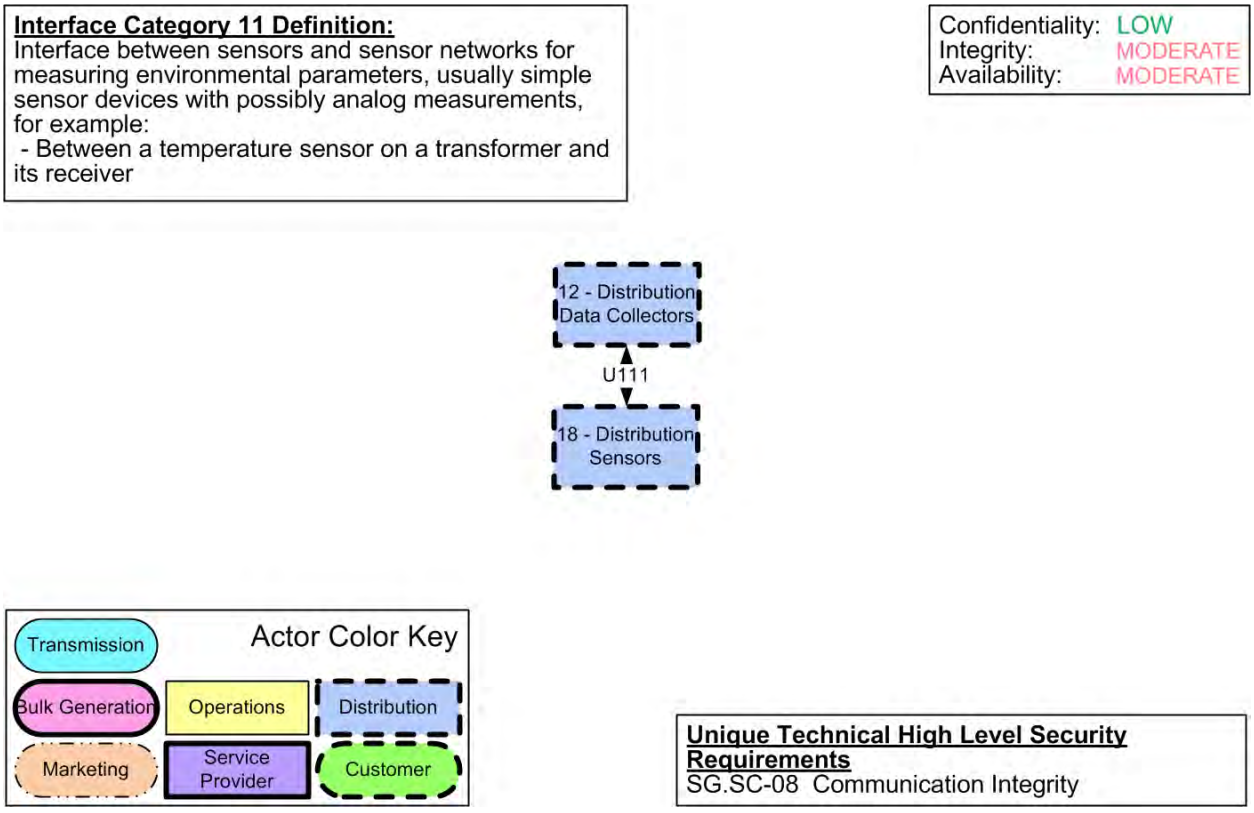

Figure 2-14 Logical Interface Category 11

2.3.8 Logical Interface Category 12: Interface between sensor networks and control systems

Logical interface category 12 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.

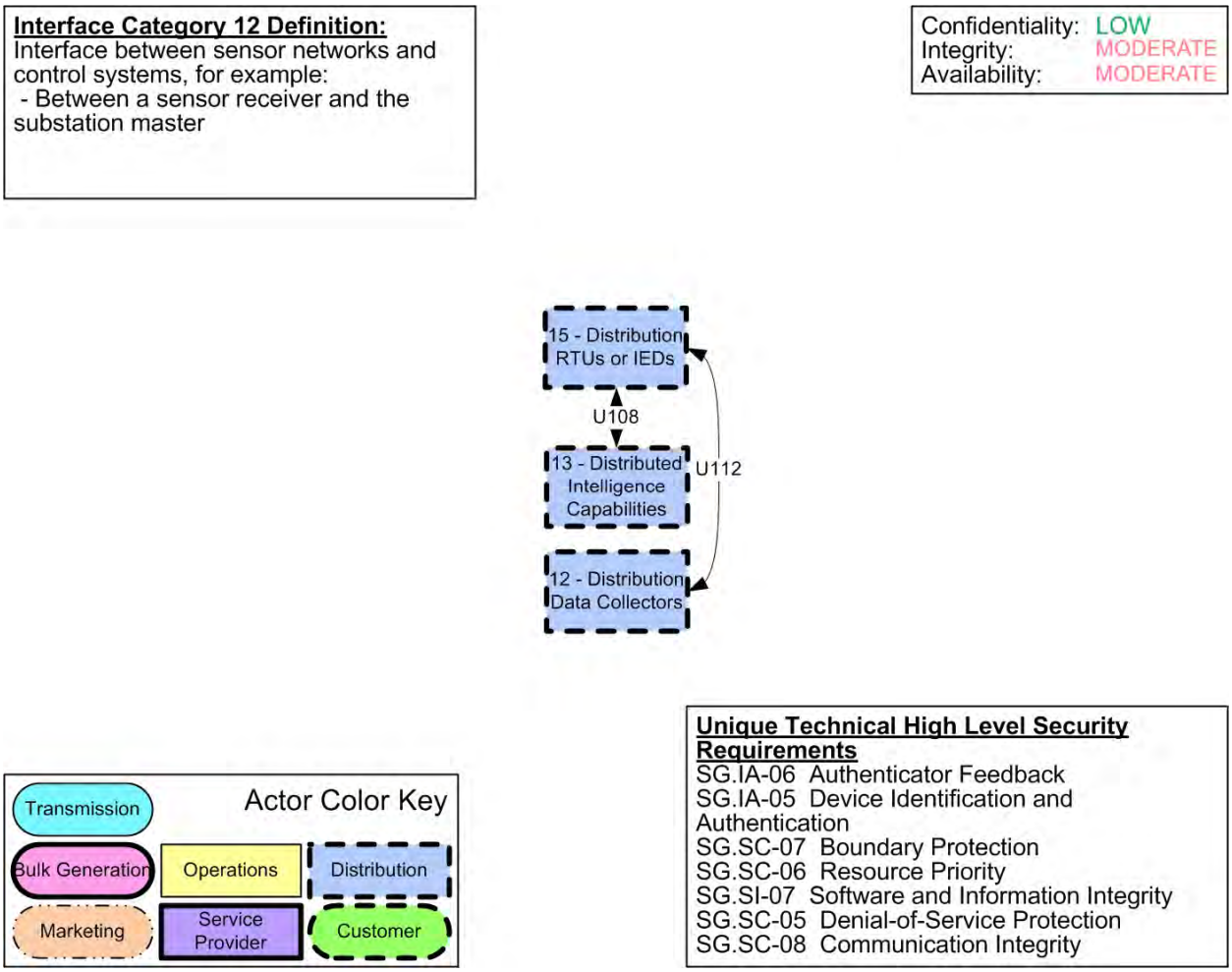

Figure 2-15 Logical Interface Category 12

2.3.9 Logical Interface Category 13: Interface between systems that use the AMI network

Logical interface category 13 covers the interfaces between systems that use the AMI network, for example:

- Between MDMS and meters; and
- 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 DoS situations.

- Meters are constrained in their computational capabilities, primarily to keep costs down, which may limit the types and layers of security that could be applied.
- Revenue-grade meters must be certified, so 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 unsecured 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.

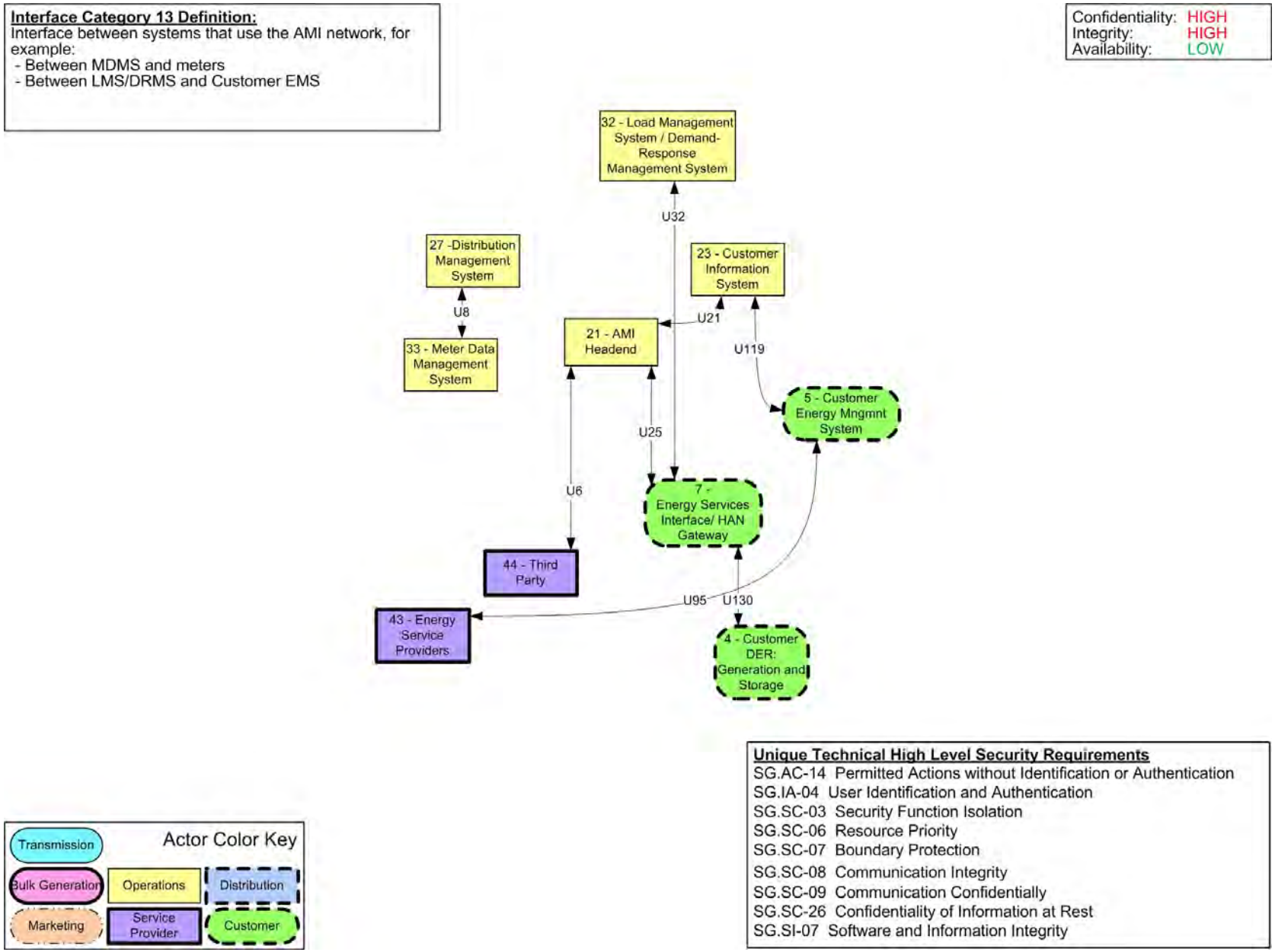

Figure 2-16 Logical Interface Category 13

2.3.10 Logical Interface Category 14: Interface between systems that use the AMI network for functions that require high availability

Logical interface category 14 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; and
- Between DMS applications and distribution automation (DA) field equipment.

Although both logical interface categories 13 and 14 use the AMI network to connect to field sites, the issues for logical interface category 14 differ from those of 13, because the interactions are focused on power operations of DER and 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 DoS 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 deployments 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, is found in unsecured 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.

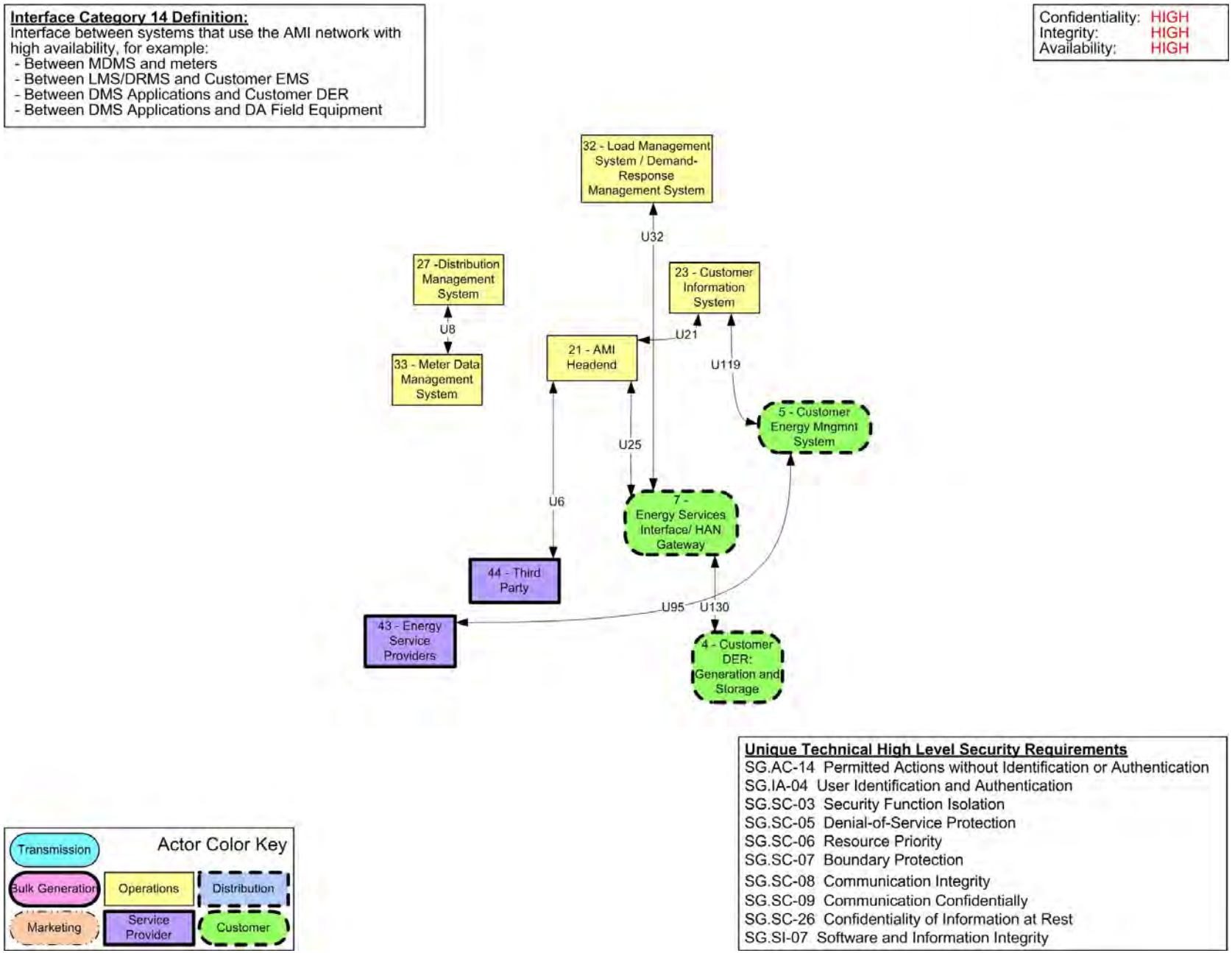

Figure 2-17 Logical Interface Category 14

2.3.11 Logical Interface Category 15: Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs

Logical interface category 15 covers the interface between systems that use customer (residential, commercial, and industrial) site networks such as home area networks, building/business area networks, and neighborhood area networks (NANs), for example:

- Between customer EMS and customer appliances;
- Between customer EMS and customer DER equipment; and
- Between an energy services interface (ESI) and PEVs.

The security-related issues for this intra-customer site environment 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 capture 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 moderate across HANs 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 media will be local wireless (e.g., Wi-Fi, 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 greater 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 that 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 HANs, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing.

- HANs 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 unsecured 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.

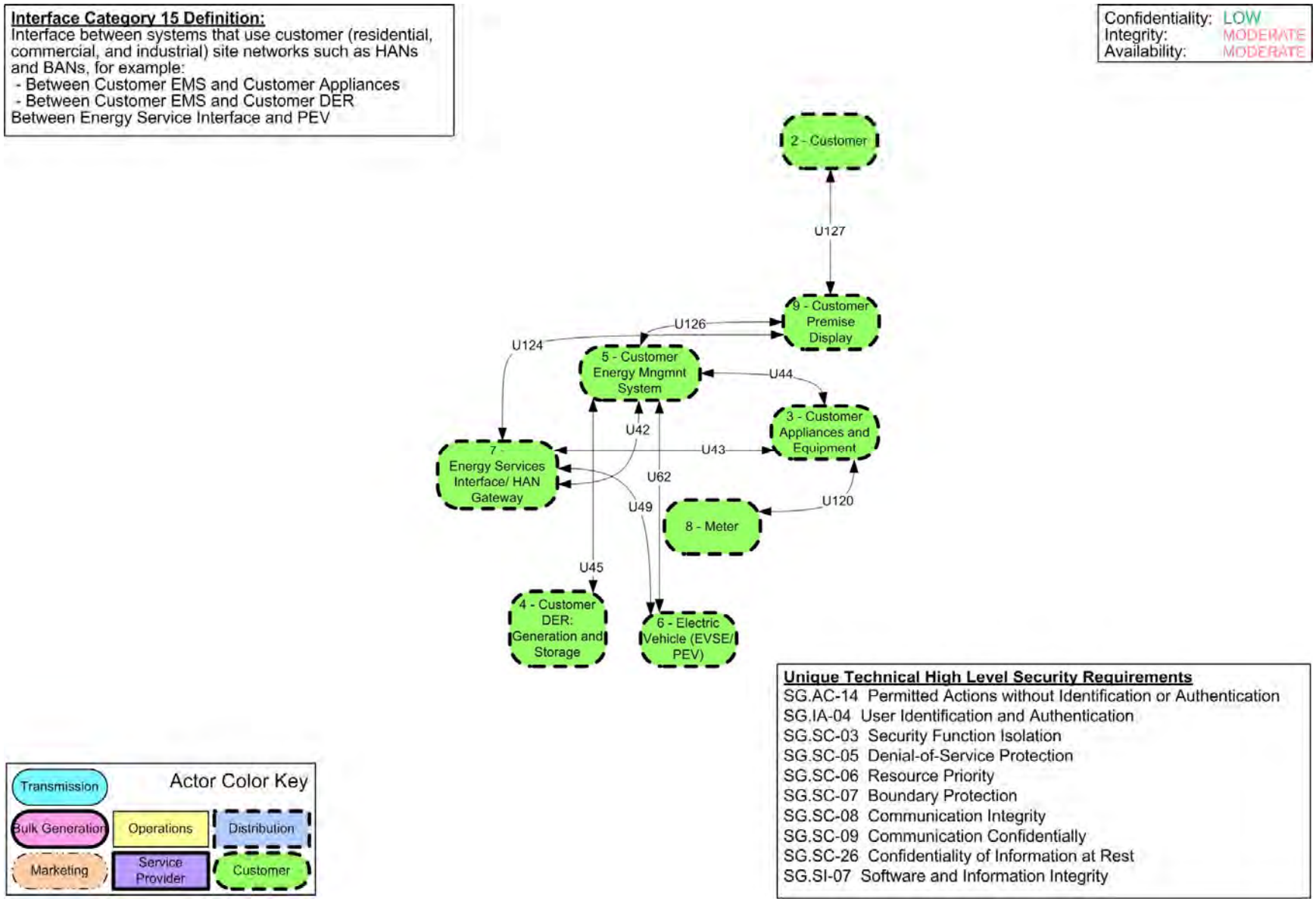

Figure 2-18 Logical Interface Category 15

2.3.12 Logical Interface Category 16: Interface between external systems and the customer site

Logical interface category 16 covers the interface between external systems and the customer site, for example:

- Between a third party and the HAN gateway;
- Between ESP and DER; and
- Between the 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 that 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 a higher volume of data traffic. Many different types of media, particularly public media, are increasingly available, including the public Internet over cable or digital subscriber line (DSL), campus or corporate intranets, cell phone general packet radio service (GPRS), and neighborhood WiMAX and Wi-Fi systems.
- Some customer devices that contain their own "HAN gateway" firewall are constrained in their computational 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 unsecured 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.

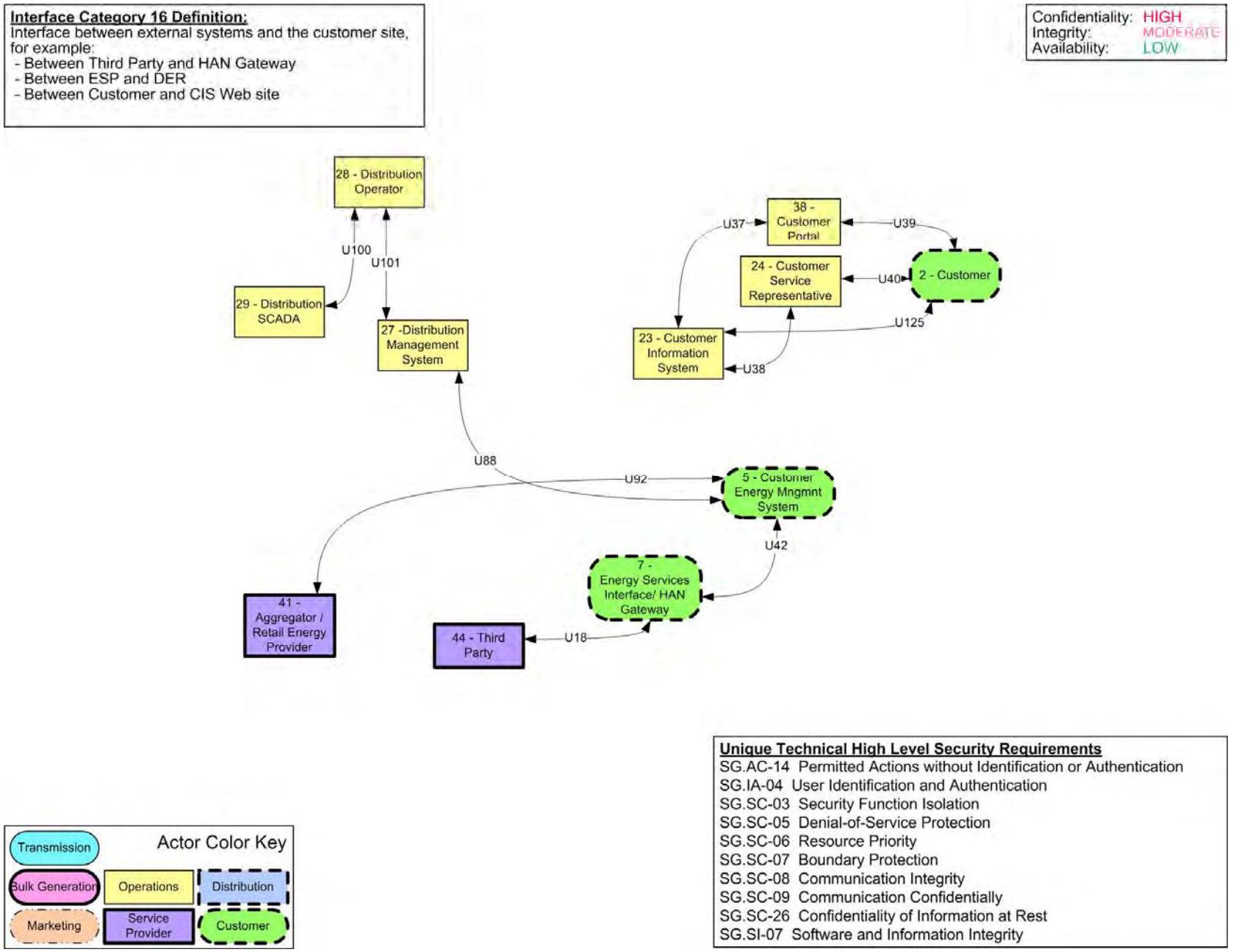

Figure 2-19 Logical Interface Category 16

2.3.13 Logical Interface Category 17: Interface between systems and mobile field crew laptops/equipment

Logical interface category 17 covers the interfaces between systems and mobile field crew laptops/equipment, for example:

- Between field crews and a GIS;
- Between field crews and CIS;
- Between field crews and substation equipment;
- Between field crews and OMS;
- Between field crews and WMS; and
- 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 laptops or personal digital assistants (PDAs) 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; and
- Obtaining customer and product information for upsell opportunities.

The key characteristics of this interface category are as follows:

- 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; and
  - 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 multivendor services are interfaced with utility systems.

- 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 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 transmitted when the volume of data is too large to transmit over a wireless connection or when the area does not have wireless coverage. In such cases, data is maintained on the laptop/PDA until it is reconnected to a physical network.
- Note: Data that is captured (e.g., metering data, local device passwords, security parameters) must be protected at the appropriate level.

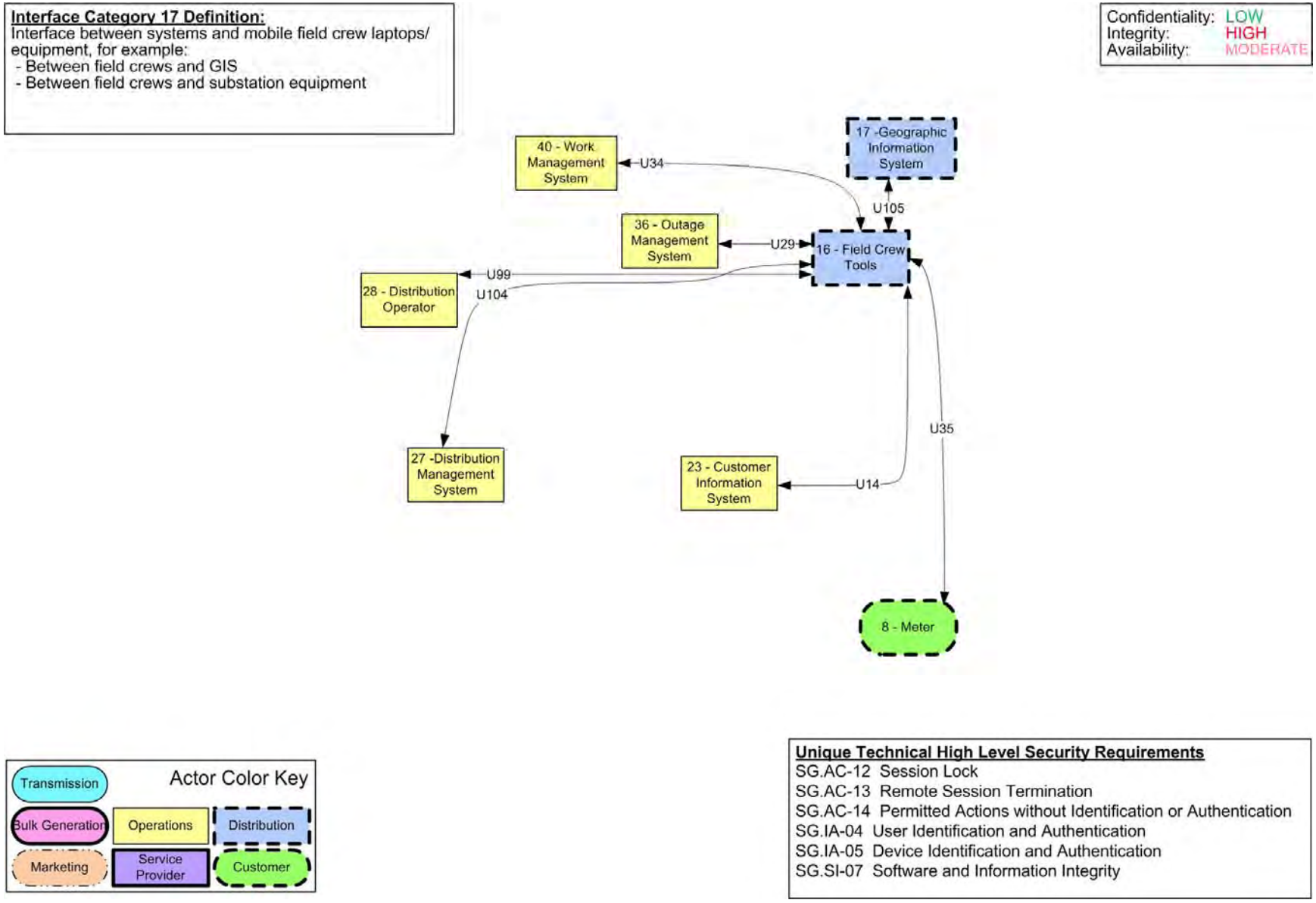

Figure 2-20 Logical Interface Category 17

2.3.14 Logical Interface Category 18: Interface between metering equipment

Logical interface category 18 covers the interface between metering equipment, for example:

- Between submeter to meter;
- Between PEV meter and ESP;
- Between MDMS and meters (via the AMI headend);
- Between customer EMS and meters;
- Between field crew tools and meters;
- Between customer DER and submeters; and
- Between electric vehicles and submeters.

The issues for this metering interface category include the following:

- 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 computational capabilities, primarily to keep costs down, which may limit the types and layers of security that could be applied.
- Revenue-grade meters must be certified, so 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 unsecured locations that are not under utility control, limiting physical security.
- Customer reactions to AMI systems and smart meters are as yet unknown.

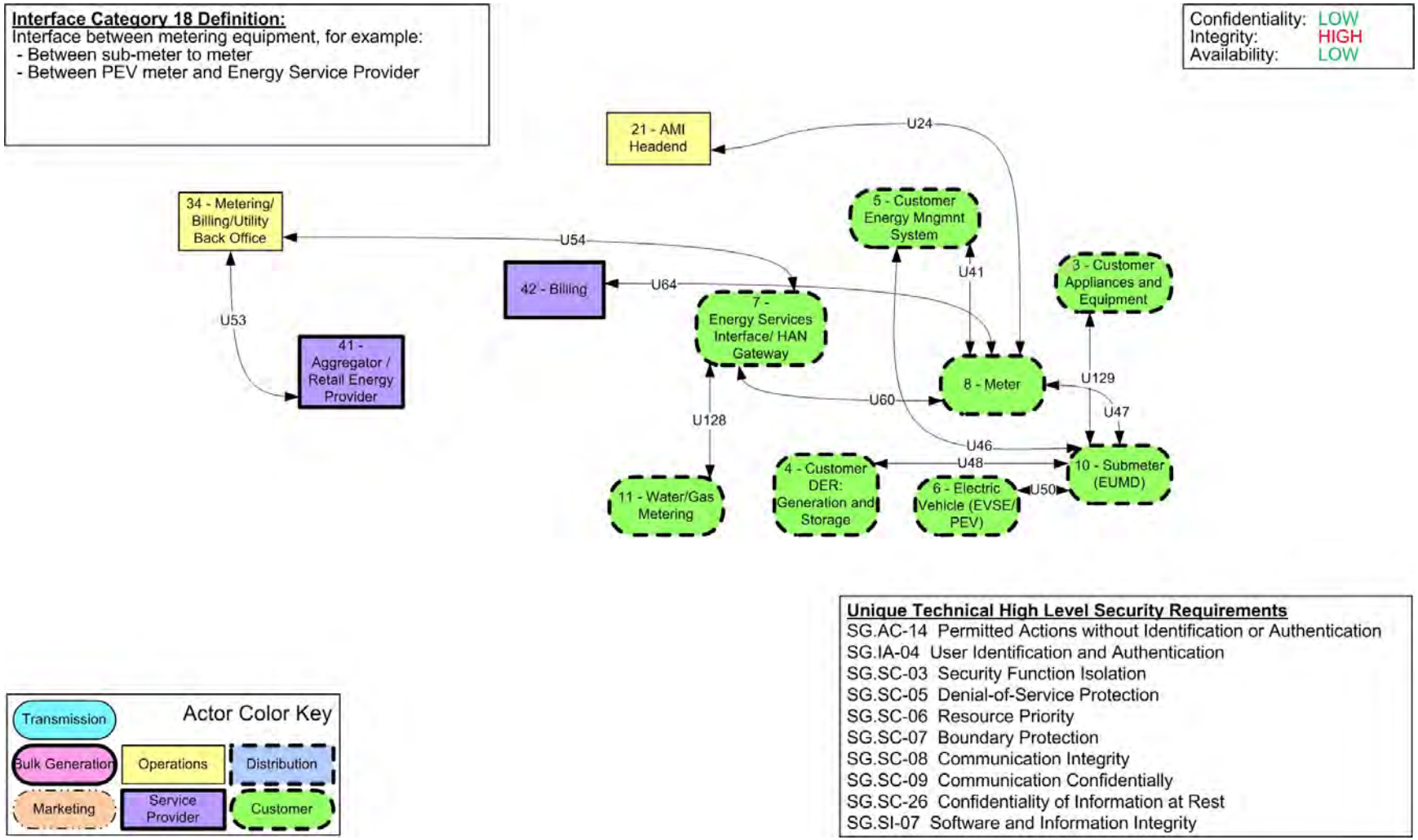

Figure 2-21 Logical Interface Category 18

2.3.15 Logical Interface Category 19: Interface between operations decision support systems

Logical interface category 19 covers the interfaces between operations decision support systems, e.g., between 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 categories 1-4).

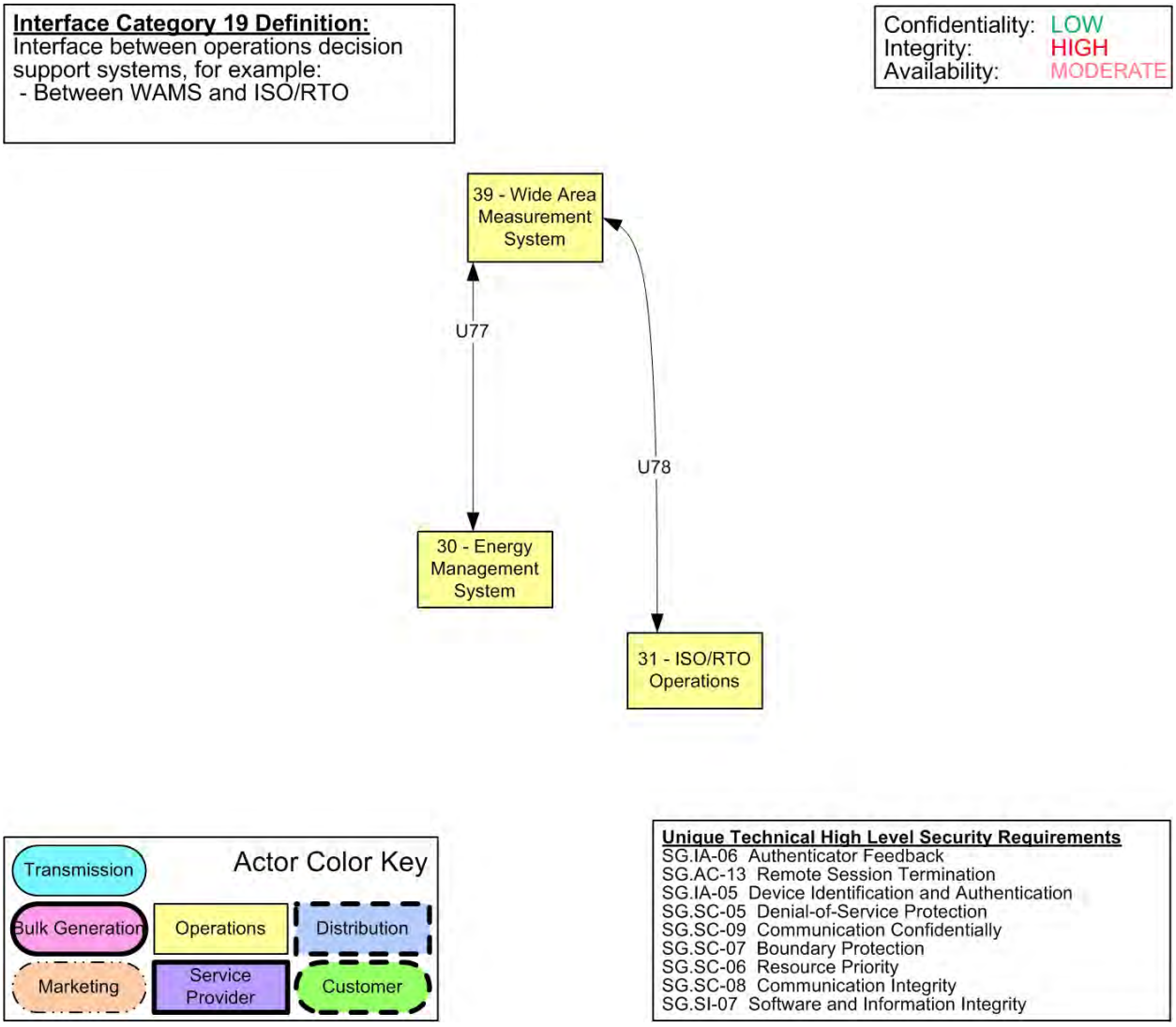

Figure 2-22 Logical Interface Category 19

2.3.16 Logical Interface Category 20: Interface between engineering/ maintenance systems and control equipment

Logical interface category 20 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; and
- Within power plants.

The main activities performed on this interface include:

- Installing and changing device settings, which 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; and
- Software updates.

The key characteristics of this interface category are as follows:

- The functions performed on this interface are not considered real-time activities.
- 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.
- 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 connection;
  - Local access at the device (addressed in Logical Interface Category 17); and
  - Access via the same interface used for real-time communications.

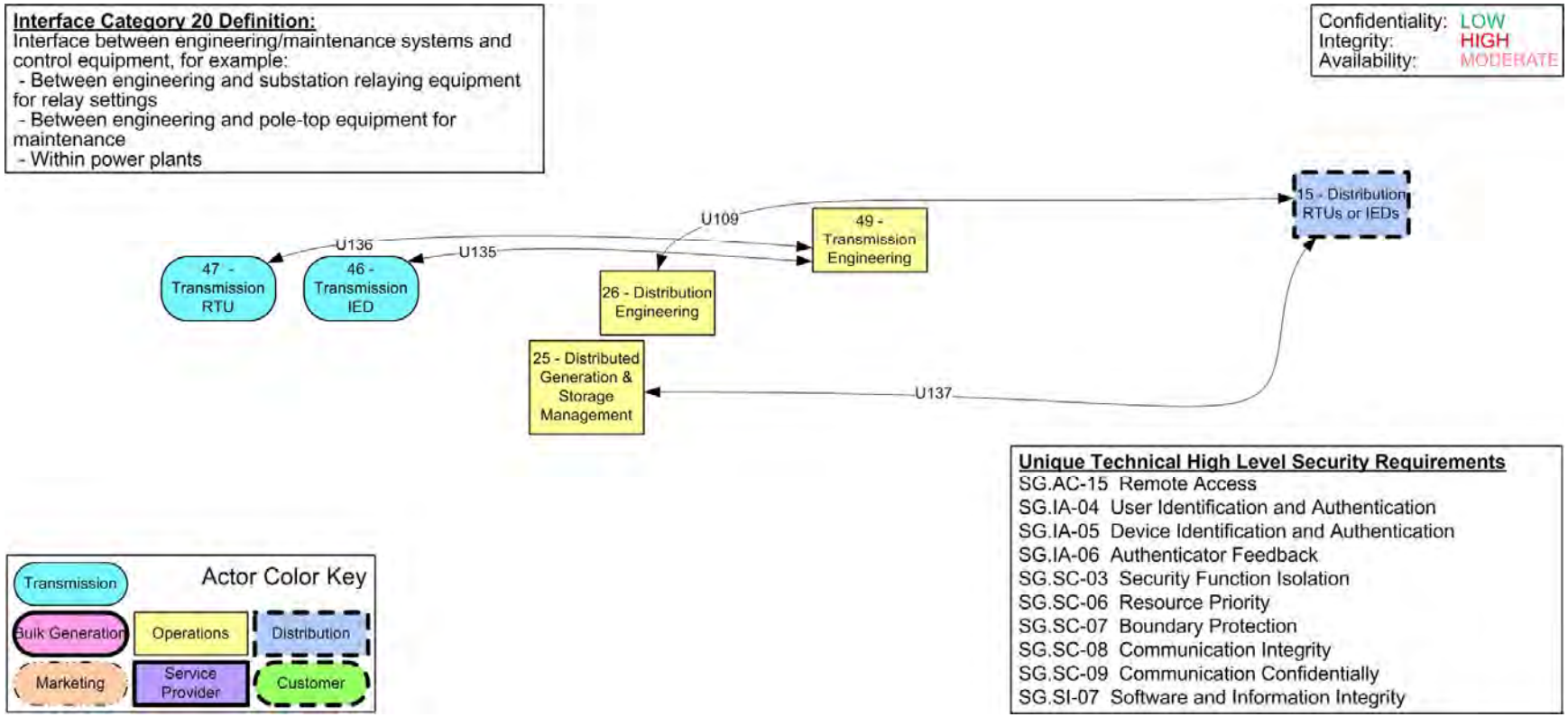

Figure 2-23 Logical Interface Category 20

2.3.17 Logical Interface Category 21: Interface between control systems and their vendors for standard maintenance and service

Logical interface category 21 covers the interfaces between control systems and their vendors for standard maintenance and service, for example:

- Between SCADA system and its vendor.

The main activities performed on this interface include:

- Updating firmware and/or software;
- Retrieving maintenance information; and
- Retrieving event logs.

Key characteristics of this logical interface category are as follows:

- The functions performed on this interface are not considered real-time activities.
- 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 connection;
  - Local access at the device/control system console; and
  - Access via the same interface used for real-time communications.

Activities outside of the scope of Logical Interface Category 21 include:

- Vendors acting in an (outsourced) operational role (see Logical Interface Categories 1-4, 5-6, or 20, depending upon the role).

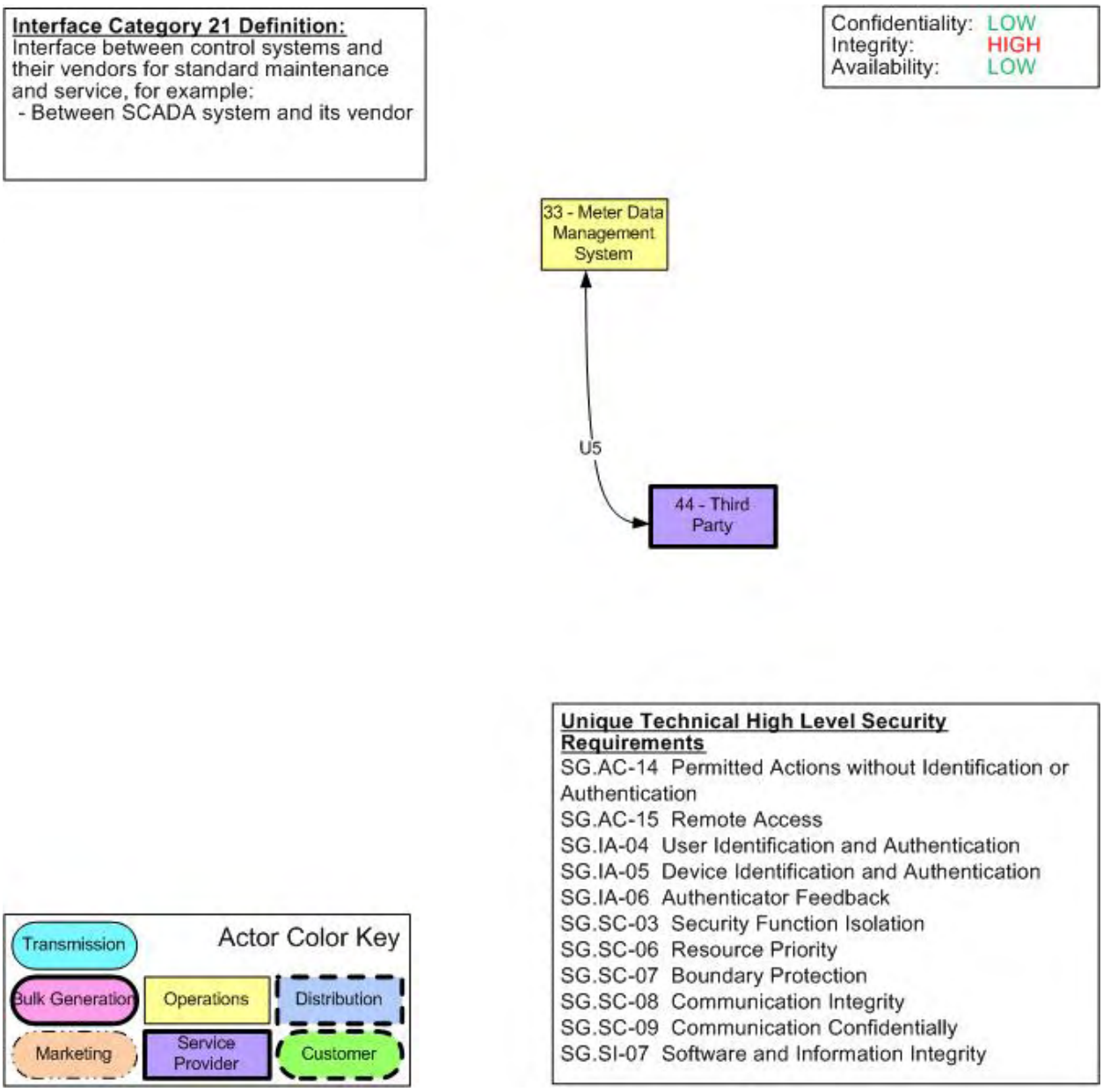

Figure 2-24 Logical Interface Category 21

2.3.18 Logical Interface Category 22: Interface between security/network/system management consoles and all networks and systems

Logical interface category 22 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 settings and audit log retrieval (if the security audit log is separate from the event logs);
- Future real-time monitoring of the security infrastructure; and
- Security infrastructure operations and maintenance.

Key characteristics of this logical interface category as follows:

- The functions performed on this interface are not considered real-time activities.
- 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 connection;
  - Local access at the device/control system console; and
  - Access via the same interface used for real-time communications.

Activities outside of the scope of Logical interface category 22 include:

- Smart Grid transmission and distribution (see Logical Interface Categories 1-4 and 5-6);
- Advanced metering (see Logical Interface Category 13); and
- Control systems engineering and systems maintenance (see Logical Interface Category 20).

(Note: This diagram is not included in the logical reference model, Figure 2-3.)

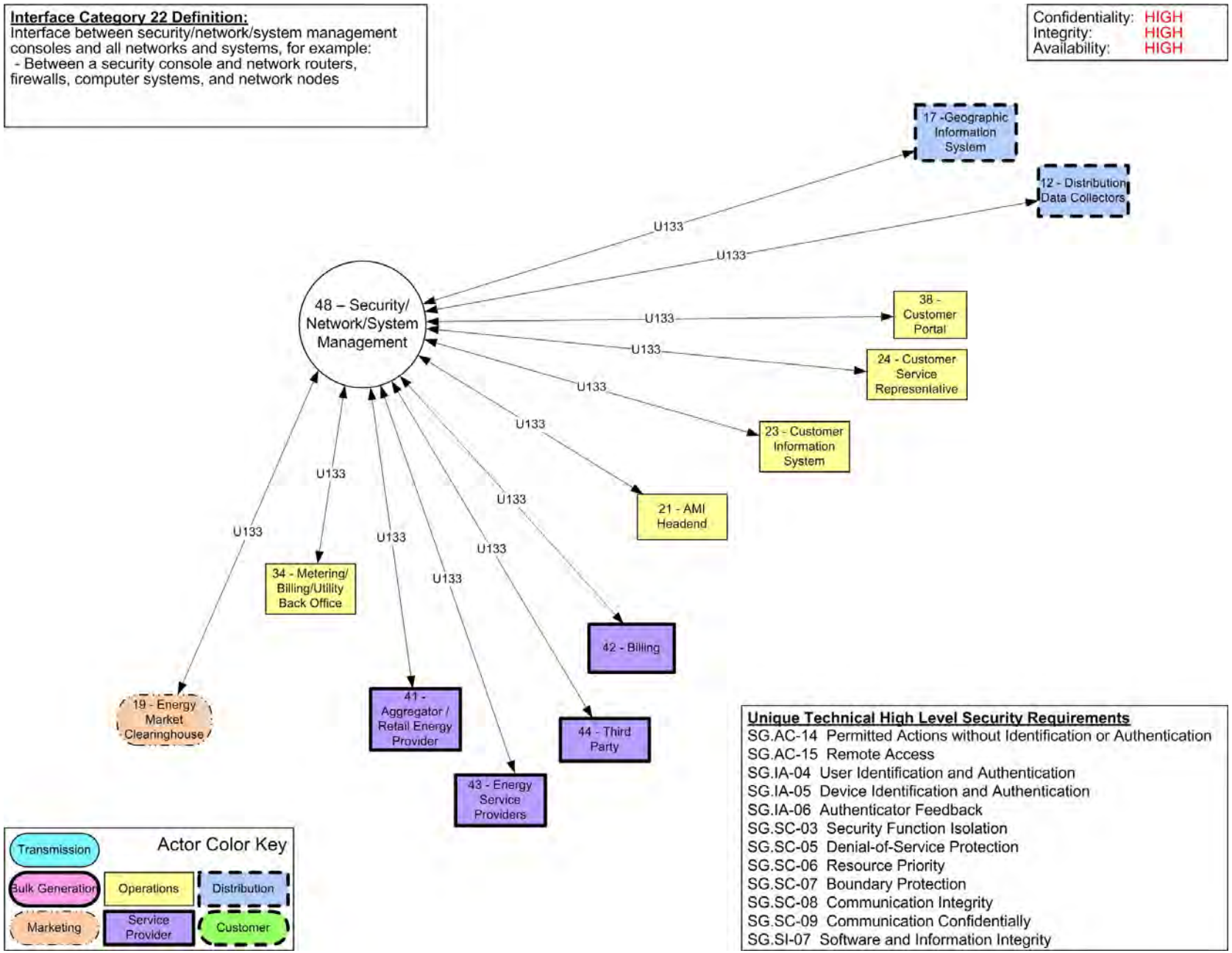

Figure 2-25 Logical Interface Category 22

CHAPTER THREE
HIGH-LEVEL SECURITY REQUIREMENTS

This chapter includes the detailed descriptions for each of the security requirements. The analyses used to select and modify these security requirements are included in Appendix G. This chapter includes the following:

1. Determination of the confidentiality, integrity, and availability (CI&A) impact levels for each of the logical interface categories. (*See* Table 3-2.)
2. The common governance, risk, and compliance (GRC), common technical, and unique technical requirements are allocated to the logical interface categories. Also, the impact levels are included for each requirement. (*See* Table 3-3.)
3. The security requirements for the Smart Grid. Included are the detailed descriptions for each requirement.

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

3.1 CYBER SECURITY OBJECTIVES

For decades, power system operations have been managing the reliability of the power grid in which power *availability* has been the primary requirement, with information integrity as a secondary but increasingly critical requirement. Confidentiality of customer information is also important in the normal revenue billing processes and for privacy concerns. 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.

Availability is the most important security objective for power system reliability. The time latency associated with availability can vary—

- ≤ 4 ms for protective relaying;
- Subseconds for transmission wide-area situational awareness monitoring;
- Seconds for substation and feeder SCADA data;
- Minutes for monitoring noncritical 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;

- Time stamp 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 CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY IMPACT LEVELS

Following are the definitions for the security objectives of CI&A, 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 in Table 3-1 as low, moderate, and high as defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. The impact levels are used in the selection of security requirements for each logical interface category.

Table 3-1 Impact Levels Definitions

	Potential Impact Levels		
	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 assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, 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.

3.3 IMPACT LEVELS FOR THE CI&A 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 here for specific logical interface categories.

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 (low [L], moderate [M], and high [H]) presented in Table 3-2 address the impacts to the nationwide power grid, particularly with regard to grid stability and reliability. Consequentially, the confidentiality impact is low for these logical interface categories. Logical interface categories 7, 8, 13, 14, 16, and 22 have a high impact level for confidentiality because of the type of data that needs to be protected (e.g., sensitive customer energy usage data, critical security parameters, and information from a HAN to a third party.)

Table 3-2 Smart Grid Impact Levels

Logical Interface Category	Confidentiality	Integrity	Availability
1	L	H	H
2	L	H	M
3	L	H	H
4	L	H	M
5	L	H	H
6	L	H	M
7	H	M	L
8	H	M	L
9	L	M	M
10	L	H	M
11	L	M	M
12	L	M	M
13	H	H	L
14	H	H	H
15	L	M	M
16	H	M	L
17	L	H	M
18	L	H	L
19	L	H	M
20	L	H	M
21	L	H	L
22	H	H	H

3.4 SELECTION OF 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 24×7 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 that 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 the compromise of an 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 organizations as they develop their cyber security strategy, perform risk assessments, and select and modify security requirements for Smart Grid information system implementations.

Additional criteria must be used in determining the cyber security requirements before selecting and implementing the cyber security measures/solutions. 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 components/devices, 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 and general enough to permit the implementation of different cyber security solutions that meet the security requirements or embrace new security technologies as they are developed. This cyber security information can then be used in subsequent steps to select security requirements for the Smart Grid.

The security requirements listed below are an amalgam from several sources: NIST SP 800-53, the DHS Catalog, NERC CIPs, and the NRC Regulatory Guidance. After the security requirements were selected, they were modified as required. The goal was to develop a set of security requirements that address the needs of the electric sector and the Smart Grid. Each security requirement is allocated to one of three categories: governance, risk, and compliance (GRC), common technical, or unique technical. The intent of the GRC requirements is to have them addressed at the organization level. It may be necessary to augment these organization-level requirements for specific logical interface categories and/or Smart Grid information systems. The common technical requirements are applicable to all of the logical interface categories. The unique technical requirements are allocated to one or more of the logical interface categories. The common and unique technical requirements should be allocated to each Smart Grid system and not necessarily to every component within a system, as the focus is on security at the system level. Each organization must develop a security architecture for each Smart Grid information system and allocate security requirements to components/devices. Some

security requirements may be allocated to one or more components/devices. However, not every security requirement must be allocated to every component/device. Table 3-3 includes only the security requirements that were selected. There are additional security requirements included in the next section that were not selected. These may be included by an organization if it determines that the security requirements are necessary to address specific risks and needs.

For each unique technical requirement, the recommended security impact level is specified (e.g., low [L], moderate [M], or high [H]). The common technical requirements and GRC requirements apply to all logical interface categories. A recommended impact level is included with each of the common technical and GRC requirements. The requirement may be the same at all impact levels. If there are additional requirements at the moderate and high impact levels, these are listed in the table. The information included in the table is a guideline and presented as a starting point for organizations as they implement Smart Grid information systems. Each organization should use this guidance information as it implements the security strategy and performs the security risk assessment.

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 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.

3.5 SECURITY REQUIREMENTS EXAMPLE

This example illustrates how to select security requirements using the material in this report. Included in this example are some GRC, common technical and unique technical requirements that may apply to a Smart Grid information system.

Example: Smart Grid control system "ABC" includes logical interface category 6: interface between control systems in different organizations. As specified in the previous chapter, this requires high data accuracy, high availability, and establishment of a chain of trust.

The organization will need to review all the GRC requirements to determine if any of these requirements need to be modified or augmented for the ABC control system. For example, SG.AC-1, Access Control Policy and Procedures, is applicable to all systems, including the ABC control system. This security requirement does not need to be revised for the ABC control system because it is applicable at the organization level. In contrast, for GRC requirement SG.CM-6, Configuration Settings, the organization determines that there are unique settings for the ABC control system.

For common technical requirement SG.SI-2, Flaw Remediation, the organization determines that the procedures already specified are applicable to the ABC control system, without modification. In contrast, for common technical requirement SG.AC-7, Least Privilege, the organization determines that a unique set of access rights and privileges are necessary for the ABC control system because the system interconnects with a system in a different organization.

Unique technical requirement SG.SI-7, Software and Information Integrity, was allocated to logical interface category 6. The organization has determined that this security requirement is important for the ABC control system, and includes it in the suite of security requirements.

3.6 RECOMMENDED SECURITY REQUIREMENTS

Table 3-3 lists the selected security requirements for the Smart Grid.

Table 3-3 Allocation of Security Requirements to Logical Interface Catgories

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Requirement Number	Logical Interface Categories																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.AC-1	Applies at all impact levels																					
SG.AC-2	Applies at all impact levels																					
SG.AC-3	Applies at all impact levels																					
SG.AC-4	Applies at all impact levels																					
SG.AC-6	Applies at moderate and high impact levels																					
SG.AC-7	Applies at moderate and high impact levels																					
SG.AC-8	Applies at all impact levels																					
SG.AC-9	Applies at all impact levels																					
SG.AC-12							H	H									L				L	H
SG.AC-13																	M		M			
SG.AC-14	H	H	H	H	H	H	M	M	M	H			H	H	M	M	H	H		H	H	H
SG.AC-15																				H	H	H
SC.AC-16	Applies at all impact levels																					
SG.AC-17	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.AC-18	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.AC-19	Applies at all impact levels																					
SG.AC-20	Applies at all impact levels																					
SG.AC-21	Applies at all impact levels																					
SG.AT-1	Applies at all impact levels																					

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)																					Light Gray = Common Technical Requirement
Smart Grid Requirement Number	**Logical Interface Categories**																				
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
SG.AT-2	Applies at all impact levels																					
SG.AT-3	Applies at all impact levels																					
SG.AT-4	Applies at all impact levels																					
SG.AT-6	Applies at all impact levels																					
SG.AT-7	Applies at all impact levels																					
SG.AU-1	Applies at all impact levels																					
SG.AU-2	Applies at all impact levels with additional requirement enhancements at high impact level																					
SG.AU-3	Applies at all impact levels																					
SG.AU-4	Applies at all impact levels																					
SG.AU-5	Applies at all impact levels with additional requirement enhancements at high impact level																					
SG.AU-6	Applies at all impact levels																					
SG.AU-7	Applies at moderate and high impact levels																					
SG.AU-8	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.AU-9	Applies at all impact levels																					
SG.AU-10	Applies at all impact levels																					
SG.AU-11	Applies at all impact levels																					
SG.AU-12	Applies at all impact levels																					
SG.AU-13	Applies at all impact levels																					
SG.AU-14	Applies at all impact levels																					
SG.AU-15	Applies at all impact levels																					

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Requirement Number	Logical Interface Categories																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.AU-16							M	M	M				H	H		M				H	H	H
SG.CA-1	Applies at all impact levels																					
SG.CA-2	Applies at all impact levels																					
SG.CA-4	Applies at all impact levels																					
SG.CA-5	Applies at all impact levels																					
SG.CA-6	Applies at all impact levels																					
SG.CM-1	Applies at all impact levels																					
SG.CM-2	Applies at all impact levels																					
SG.CM-3	Applies at moderate and high impact levels																					
SG.CM-4	Applies at all impact levels																					
SG.CM-5	Applies at moderate and high impact levels																					
SG.CM-6	Applies at all impact levels																					
SG.CM-7	Applies at all impact levels																					
SG.CM-8	Applies at all impact levels																					
SG.CM-9	Applies at all impact levels																					
SG.CM-10	Applies at all impact levels																					
SG.CM-11	Applies at all impact levels																					
SG.CP-1	Applies at all impact levels																					

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Requirement Number	Logical Interface Categories																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.CP-2	Applies at all impact levels																					
SG.CP-3	Applies at all impact levels																					
SG.CP-4	Applies at all impact levels																					
SG.CP-5	Applies at moderate and high impact levels																					
SG.CP-6	Applies at all impact levels																					
SG.CP-7	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.CP-8	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.CP-9	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.CP-10	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.CP-11	Applies at high impact levels																					
SG.IA-1	Applies at all impact levels																					
SG.IA-2	Applies at all impact levels																					
SG.IA-3	Applies at all impact levels																					
SG.IA-4	H	H	H	H	H	H	M	M	M	H			H	H	M	M	H	H		H	H	H
SG.IA-5	H	H	H	H			M	M				M					H		H	H	H	H
SG.IA-6	L	L	L	L	L	L	H	H	L	L			H	H	L	H	L	L		L	L	H
SG.ID-1	Applies at all impact levels																					
SG.ID-2	Applies at all impact levels																					

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)	Light Gray = Common Technical Requirement

Smart Grid Requirement Number	Logical Interface Categories																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.ID-3	Applies at all impact levels																					
SG.ID-4	Applies at all impact levels																					
SG.IR-1	Applies at all impact levels																					
SG.IR-2	Applies at all impact levels																					
SG.IR-3	Applies at all impact levels																					
SG.IR-4	Applies at all impact levels																					
SG.IR-5	Applies at all impact levels																					
SG.IR-6	Applies at all impact levels																					
SG.IR-7	Applies at all impact levels																					
SG.IR-8	Applies at all impact levels																					
SG.IR-9	Applies at all impact levels																					
SG.IR-10	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.IR-11	Applies at all impact levels																					
SG.MA-1	Applies at all impact levels																					
SG.MA-2	Applies at all impact levels																					
SG.MA-3	Applies at all impact levels with additional requirement enhancements at high impact levels																					
SG.MA-4	Applies at all impact levels																					
SG.MA-5	Applies at all impact levels																					
SG.MA-6	Applies at all impact levels with additional requirement enhancements at high impact levels																					

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)																					Light Gray = Common Technical Requirement
Smart Grid Requirement Number	**Logical Interface Categories**																				
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
SG.MA-7	Applies at all impact levels																					
SG.MP-1	Applies at all impact levels																					
SG.MP-2	Applies at all impact levels																					
SG.MP-3	Applies at moderate and high impact levels																					
SG.MP-4	Applies at all impact levels																					
SG.MP-5	Applies at all impact levels																					
SG.MP-6	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.PE-1	Applies at all impact levels																					
SG.PE-2	Applies at all impact levels																					
SG.PE-3	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.PE-4	Applies at all impact levels																					
SG.PE-5	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.PE-6	Applies at all impact levels																					
SG.PE-7	Applies at all impact levels																					
SG.PE-8	Applies at all impact levels																					
SG.PE-9	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.PE-10	Applies at all impact levels																					
SG.PE-11	Applies at all impact levels																					
SG.PE-12	Applies at all impact levels with additional requirement enhancements at high impact level																					

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)																						
Light Gray = Common Technical Requirement																						
Smart Grid Requirement Number	**Logical Interface Categories**																					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
SG.PL-1	Applies at all impact levels																					
SG.PL-2	Applies at all impact levels																					
SG.PL-3	Applies at all impact levels																					
SG.PL-4	Applies at all impact levels																					
SG.PL-5	Applies at all impact levels																					
SG.PM-1	Applies at all impact levels																					
SG.PM-2	Applies at all impact levels																					
SG.PM-3	Applies at all impact levels																					
SG.PM-4	Applies at all impact levels																					
SG.PM-5	Applies at all impact levels																					
SG.PM-6	Applies at all impact levels																					
SG.PM-7	Applies at all impact levels																					
SG.PM-8	Applies at all impact levels																					
SG.PS-1	Applies at all impact levels																					
SG.PS-2	Applies at all impact levels																					
SG.PS-3	Applies at all impact levels																					
SG.PS-4	Applies at all impact levels																					
SG.PS-5	Applies at all impact levels																					
SG.PS-6	Applies at all impact levels																					

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)	Light Gray = Common Technical Requirement

Smart Grid Requirement Number	Logical Interface Categories																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.PS-7	Applies at all impact levels																					
SG.PS-8	Applies at all impact levels																					
SG.PS-9	Applies at all impact levels																					
SG.RA-1	Applies at all impact levels																					
SG.RA-2	Applies at all impact levels																					
SG.RA-3	Applies at all impact levels																					
SG.RA-4	Applies at all impact levels																					
SG.RA-5	Applies at all impact levels																					
SG.RA-6	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.SA-1	Applies at all impact levels																					
SG.SA-2	Applies at all impact levels																					
SG.SA-3	Applies at all impact levels																					
SG.SA-4	Applies at all impact levels																					
SG.SA-5	Applies at all impact levels																					
SG.SA-6	Applies at all impact levels																					
SG.SA-7	Applies at all impact levels																					
SG.SA-8	Applies at all impact levels																					
SG.SA-9	Applies at all impact levels																					
SG.SA-10	Applies at all impact levels																					

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Requirement Number	Logical Interface Categories																					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
SG.SA-11	Applies at all impact levels																					
SG.SC-1	Applies at all impact levels																					
SG.SC-3	H	H	H	H			M	M					H	H	M	M		H		H	H	H
SG.SC-5	H	M	H	M	M	M			M	M		M		H	M				M			H
SG.SC-6					H									H								H
SG.SC-7	H	H	H	H	H	H		M	M	H		M	H	H	M	M		H	H	H	H	H
SG.SC-8	H	H	H	H	H	H	M	M	M	H	M	M	H	H	M	M		H	H	H	H	H
SG.SC-9													H	H		H						H
SG.SC-11	Applies at all impact levels with additional requirement enhancements at high impact levels																					
SG.SC-12	Applies at all impact levels																					
SG.SC-13	Applies at all impact levels																					
SG.SC-15	Applies at all impact levels																					
SG.SC-16	Applies at moderate and high impact levels																					
SG.SC-18	Applies at all impact levels																					
SG.SC-19	Applies at all impact levels																					
SG.SC-20	Applies at all impact levels																					
SG.SC-21	Applies at all impact levels																					
SG.SC-22	Applies at moderate and high impact levels																					
SG.SC-26							H	H					H	H		H						H
SG.SC-29	H	H	H	H	H	H				H			H	H			H	H	H	H	H	H

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Requirement Number	Logical Interface Categories																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.SC-30	Applies at moderate and high impact levels																					
SG.SI-1	Applies at all impact levels																					
SG.SI-2	Applies at all impact levels																					
SG.SI-3	Applies at all impact levels																					
SG.SI-4	Applies at all impact levels																					
SG.SI-5	Applies at all impact levels																					
SG.SI-6	Applies at moderate and high impact levels																					
SG.SI-7	H	H	H	H	H	H	M	M	M	H		M	H	H	M	M	H	H	H	H	H	H
SG.SI-8	Applies at moderate and high impact levels																					
SG.SI-9	Applies at all impact levels																					

3.6.1 Security Requirements

This section contains the recommended security requirements for the Smart Grid. The recommended security requirements are organized into families primarily based on NIST SP 800-53. A cross-reference of the Smart Grid security requirements to NIST SP 800-53, the DHS Catalog, and the NERC CIPs is included in Appendix A.

The following information is included with each security requirement:

1. Security requirement identifier and name. Each security requirement has a unique identifier that consists of three components. The initial component is SG – for Smart Grid. The second component is the family name, e.g., AC for access control and CP for Continuity of Operations. The third component is a unique numeric identifier, for example, SG.AC-1 and SG.CP-3. Each requirement also has a unique name.
2. Category. Identifies whether the security requirement is a GRC, common technical, or unique technical requirement. For each common technical security requirement, the most applicable objective (confidentiality, integrity, and availability) is listed.
3. The *Requirement* describes specific security-related activities or actions to be carried out by the organization or by the Smart Grid information system.
4. The *Supplemental Guidance* section provides additional information that may be useful in understanding the security requirement. This information is guidance and is not part of the security requirement.
5. The *Requirement Enhancements* provide statements of security capability to (i) build additional functionality in a requirement, and/or (ii) increase the strength of a requirement. In both cases, the requirement enhancements are used in a Smart Grid information system requiring greater protection due to the potential impact of loss based on the results of a risk assessment. Requirement enhancements are numbered sequentially within each requirement.
6. The *Additional Considerations* provide additional statements of security capability that may be used to enhance the associated security requirement. These are provided for organizations to consider as they implement Smart Grid information systems and are not intended as security requirements. Each additional consideration is number A1, A2, etc., to distinguish them from the security requirements and requirement enhancements.
7. The *Impact Level Allocation* identifies the security requirement and requirement enhancements, as applicable, at each impact level: low, moderate, and high. The impact levels for a specific Smart Grid information system will be determined by the organization in the risk assessment process.

The term *information* is used to include data that is received and data that is sent—including, for example, data that is interpreted as a command, a setting, or a request to send data.

The requirements related to emergency lighting, fire protection, temperature and humidity controls, water damage, power equipment and power cabling, and lockout/tagout[21] are important

[21] Lockout/tagout is a safety procedure which is used in industry to ensure that dangerous machines are properly shut off and not started up again prior to the completion of maintenance or servicing work.

requirements for safety. These are outside the scope of cyber security and are not included in this report. However, these requirements must be addressed by each organization in accordance with local, state, federal, and organizational regulations, policies, and procedures.

The requirements related to privacy are not included in this chapter. They are included in Chapter 5 of this report. Specifically, privacy principle recommendations based on the PIA are included in §5.4.2, Summary PIA Findings and Recommendations, and in §5.8, Smart Grid Privacy Summary and Recommendations.

3.7 ACCESS CONTROL (SG.AC)

The focus of access control is ensuring that resources are accessed only by the appropriate personnel, and that personnel are correctly identified. Mechanisms need to be in place to monitor access activities for inappropriate activity.

SG.AC-1 Access Control Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented access control security policy that addresses—
      i. The objectives, roles, and responsibilities for the access control security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the access control security program as it applies to all of the organizational staff, contractors, and third parties.
   b. Procedures to address the implementation of the access control security policy and associated access control protection requirements.
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the access control security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-1	Moderate: SG.AC-1	High: SG.AC-1

SG.AC-2 Remote Access Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Documents allowed methods of remote access to the Smart Grid information system;
2. Establishes usage restrictions and implementation guidance for each allowed remote access method;
3. Authorizes remote access to the Smart Grid information system prior to connection; and
4. Enforces requirements for remote connections to the Smart Grid information system.

Supplemental Guidance

Remote access is any access to an organizational Smart Grid information system by a user (or process acting on behalf of a user) communicating through an external, non-organization-controlled network (e.g., the Internet).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-2	Moderate: SG.AC-2	High: SG.AC-2

SG.AC-3 Account Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization manages Smart Grid information system accounts, including:

Authorizing, establishing, activating, modifying, disabling, and removing accounts;

1. Specifying account types, access rights, and privileges (e.g., individual, group, system, guest, anonymous and temporary);
2. Reviewing accounts on an organization-defined frequency; and
3. Notifying account managers when Smart Grid information system users are terminated, transferred, or Smart Grid information system usage changes.

Management approval is required prior to establishing accounts.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization reviews currently active Smart Grid information system accounts on an organization-defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy.

A2. The organization authorizes and monitors the use of guest/anonymous accounts.

A3. The organization employs automated mechanisms to support the management of Smart Grid information system accounts.

A4. The Smart Grid information system automatically terminates temporary and emergency accounts after an organization-defined time period for each type of account.

A5. The Smart Grid information system automatically disables inactive accounts after an organization-defined time period.

A6. The Smart Grid information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.

Impact Level Allocation

Low: SG.AC-3	Moderate: SG.AC-3	High: SG.AC-3

SG.AC-4 Access Enforcement

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system enforces assigned authorizations for controlling access to the Smart Grid information system in accordance with organization-defined policy.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization considers the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies.

Impact Level Allocation

Low: SG.AC-4	Moderate: SG.AC-4	High: SG.AC-4

SG.AC-5 Information Flow Enforcement

Category: Unique Technical Requirements

Requirement

The Smart Grid information system enforces assigned authorizations for controlling the flow of information within the Smart Grid information system and between interconnected Smart Grid information systems in accordance with applicable policy.

Supplemental Guidance

Information flow control regulates where information is allowed to travel within a Smart Grid information system and between Smart Grid information systems. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict Smart Grid information system services or provide a packet-filtering capability.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system enforces information flow control using explicit labels on information, source, and destination objects as a basis for flow control decisions.

A2. The Smart Grid information system enforces dynamic information flow control allowing or disallowing information flows based on changing conditions or operational considerations.

A3. The Smart Grid information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions.

A4. The Smart Grid information system enforces the use of human review for organization-defined security policy filters when the Smart Grid information system is not capable of making an information flow control decision.

A5. The Smart Grid information system provides the capability for a privileged administrator to configure, enable, and disable the organization-defined security policy filters.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.AC-6 Separation of Duties

Category: Common Technical Requirements, Integrity

Requirement

The organization—

1. Establishes and documents divisions of responsibility and separates functions as needed to eliminate conflicts of interest and to ensure independence in the responsibilities and functions of individuals/roles;
2. Enforces separation of Smart Grid information system functions through assigned access authorizations; and

3. Restricts security functions to the least amount of users necessary to ensure the security of the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-6	High: SG.AC-6

SG.AC-7 Least Privilege

Category: Common Technical Requirements, Integrity

Requirement

1. The organization assigns the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks; and
2. The organization configures the Smart Grid information system to enforce the most restrictive set of rights and privileges or access needed by users.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization authorizes network access to organization-defined privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system.

A2. The organization authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-7	High: SG.AC-7

SG.AC-8 Unsuccessful Login Attempts

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period.

Supplemental Guidance

Because of the potential for denial of service, automatic lockouts initiated by the Smart Grid information system are usually temporary and automatically released after a predetermined time period established by the organization. Permanent automatic lockouts initiated by a Smart Grid information system must be carefully considered before being used because of safety considerations and the potential for denial of service.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded; and

A2. If a Smart Grid information system cannot perform account/node locking or delayed logins because of significant adverse impact on performance, safety, or reliability, the system employs alternative requirements or countermeasures that include the following:

a. Real-time logging and recording of unsuccessful login attempts; and

b. Real-time alerting of a management authority for the Smart Grid information system when the number of defined consecutive invalid access attempts is exceeded.

Impact Level Allocation

Low: SG.AC-8	Moderate: SG.AC-8	High: SG.AC-8

SG.AC-9 Smart Grid Information System Use Notification

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system displays an approved system use notification message or banner before granting access to the Smart Grid information system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance.

Supplemental Guidance

Smart Grid information system use notification messages can be implemented in the form of warning banners displayed when individuals log in to the Smart Grid information system. Smart Grid information system use notification is intended only for Smart Grid information system access that includes an interactive interface with a human user and is not intended to call for such an interface when the interface does not currently exist.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-9	Moderate: SG.AC-9	High: SG.AC-9

SG.AC-10 Previous Logon Notification

Category: Unique Technical Requirements

Requirement

The Smart Grid information system notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.AC-11 Concurrent Session Control

Category: Unique Technical Requirements

Requirement

The organization limits the number of concurrent sessions for any user on the Smart Grid information system.

Supplemental Guidance

The organization may define the maximum number of concurrent sessions for a Smart Grid information system account globally, by account type, by account, or a combination. This requirement addresses concurrent sessions for a given Smart Grid information system account and does not address concurrent sessions by a single user via multiple Smart Grid information system accounts.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-11	High: SG.AC-11

SG.AC-12 Session Lock

Category: Unique Technical Requirements

Requirement

The Smart Grid information system—

1. Prevents further access to the Smart Grid information system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance

A session lock is not a substitute for logging out of the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-12	High: SG.AC-12

SG.AC-13 Remote Session Termination

Category: Unique Technical Requirements

Requirement

The Smart Grid information system terminates a remote session at the end of the session or after an organization-defined time period of inactivity.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. Automatic session termination applies to local and remote sessions.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-13	High: SG.AC-13

SG.AC-14 Permitted Actions without Identification or Authentication

Category: Unique Technical Requirements

Requirement

1. The organization identifies and documents specific user actions, if any, that can be performed on the Smart Grid information system without identification or authentication; and
2. Organizations identify any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed.

Supplemental Guidance

The organization may allow limited user actions without identification and authentication (e.g., when individuals access public Web sites or other publicly accessible Smart Grid information systems.

Requirement Enhancements

1. The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-14	Moderate: SG.AC-14 (1)	High: SG.AC-14 (1)

SG.AC-15 Remote Access

Category: Unique Technical Requirements

Requirement

The organization authorizes, monitors, and manages all methods of remote access to the Smart Grid information system.

Supplemental Guidance

Remote access is any access to a Smart Grid information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Requirement Enhancements

1. The organization authenticates remote access, and uses cryptography to protect the confidentiality and integrity of remote access sessions;
2. The Smart Grid information system routes all remote accesses through a limited number of managed access control points;
3. The Smart Grid information system protects wireless access to the Smart Grid information system using authentication and encryption. Note: Authentication applies to user, device, or both as necessary; and
4. The organization monitors for unauthorized remote connections to the Smart Grid information system, including scanning for unauthorized wireless access points on an

organization-defined frequency and takes appropriate action if an unauthorized connection is discovered.

Additional Considerations

A1. Remote access to Smart Grid information system component locations (e.g., control center, field locations) is enabled only when necessary, approved, authenticated, and for the duration necessary;

A2. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods;

A3. The organization authorizes remote access for privileged commands and security-relevant information only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system; and

A4. The organization disables, when not intended for use, wireless networking capabilities internally embedded within Smart Grid information system components.

Impact Level Allocation

Low: SG.AC-15	Moderate: SG.AC-15 (1), (2), (3), (4)	High: SG.AC-15 (1), (2), (3), (4)

SG.AC-16 Wireless Access Restrictions

Category: Common Technical Requirements, Confidentiality

Requirement

The organization—

1. Establishes use restrictions and implementation guidance for wireless technologies; and
2. Authorizes, monitors, and manages wireless access to the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization uses authentication and encryption to protect wireless access to the Smart Grid information system; and

A2. The organization scans for unauthorized wireless access points at an organization-defined frequency and takes appropriate action if such access points are discovered.

Impact Level Allocation

Low: SG.AC-16	Moderate: SG.AC-16	High: SG.AC-16

SG.AC-17 Access Control for Portable and Mobile Devices

Category: Common Technical Requirements, Confidentiality

Requirement

The organization—

1. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices, including the use of writeable, removable media and personally owned removable media;
2. Authorizes connection of mobile devices to Smart Grid information systems;
3. Monitors for unauthorized connections of mobile devices to Smart Grid information systems; and
4. Enforces requirements for the connection of mobile devices to Smart Grid information systems.

Supplemental Guidance

Specially configured mobile devices include computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel to locations that the organization determines to be of significant risk, include examining the device for signs of physical tampering and purging/reimaging the hard disk drive.

Requirement Enhancements

The organization—

1. Controls the use of writable, removable media in Smart Grid information systems;
2. Controls the use of personally owned, removable media in Smart Grid information systems;
3. Issues specially configured mobile devices to individuals traveling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; and
4. Applies specified measures to mobile devices returning from locations that the organization determines to be of significant risk in accordance with organizational policies and procedures.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-17	Moderate: SG.AC-17 (1), (2)	High: SG.AC-17 (1), (2), (3), (4)

SG.AC-18 Use of External Information Control Systems

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes terms and conditions for authorized individuals to—

1. Access the Smart Grid information system from an external information system; and

2. Process, store, and transmit organization-controlled information using an external information system.

Supplemental Guidance

External information systems are information systems or components of information systems that are outside the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of security requirements or the assessment of security requirement effectiveness.

Requirement Enhancements

1. The organization imposes restrictions on authorized individuals with regard to the use of organization-controlled removable media on external information systems.

Additional Considerations

A1. The organization prohibits authorized individuals from using an external information system to access the Smart Grid information system or to process, store, or transmit organization-controlled information except in situations where the organization (a) can verify the implementation of required security controls on the external information system as specified in the organization's security policy and security plan, or (b) has approved Smart Grid information system connection or processing agreements with the organizational entity hosting the external information system.

Impact Level Allocation

Low: SG.AC-18	Moderate: SG.AC-18 (1)	High: SG.AC-18 (1)

SG.AC-19 Control System Access Restrictions

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization employs mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization's enterprise network.

Supplemental Guidance

Access to the Smart Grid information system to satisfy business requirements needs to be limited to read-only access.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-19	Moderate: SG.AC-19	High: SG.AC-19

SG.AC-20 Publicly Accessible Content

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Designates individuals authorized to post information onto an organizational information system that is publicly accessible;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;
4. Reviews the content on the publicly accessible organizational information system for nonpublic information on an organization-defined frequency; and
5. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

Supplemental Guidance

Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This requirement addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-20	Moderate: SG.AC-20	High: SG.AC-20

SG.AC-21 Passwords

Category: Common Technical Requirements, Integrity

Requirement

1. The organization develops and enforces policies and procedures for Smart Grid information system users concerning the generation and use of passwords;
2. These policies stipulate rules of complexity, based on the criticality level of the Smart Grid information system to be accessed; and
3. Passwords shall be changed regularly and are revoked after an extended period of inactivity.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-21	Moderate: SG.AC-21	High: SG.AC-21

3.8 AWARENESS AND TRAINING (SG.AT)

Smart Grid information system security awareness is a critical part of Smart Grid information system incident prevention. Implementing a Smart Grid information system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals' roles and responsibilities.

SG.AT-1 Awareness and Training Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented awareness and training security policy that addresses—
      i. The objectives, roles, and responsibilities for the awareness and training security program as it relates to protecting the organization's personnel and assets, and
      ii. The scope of the awareness and training security program as it applies to all of the organizational staff, contractors, and third parties.
   b. Procedures to address the implementation of the awareness and training security policy and associated awareness and training protection requirements.
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the awareness and training security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-1	Moderate: SG.AT-1	High: SG.AT-1

SG.AT-2 Security Awareness

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides basic security awareness briefings to all Smart Grid information system users (including employees, contractors, and third parties) on an organization-defined frequency.

Supplemental Guidance

The organization determines the content of security awareness briefings based on the specific requirements of the organization and the Smart Grid information system to which personnel have authorized access.

Requirement Enhancements

None.

Additional Considerations

A1. All Smart Grid information system design and procedure changes need to be reviewed by the organization for inclusion in the organization security awareness training; and

A2. The organization includes practical exercises in security awareness briefings that simulate actual cyber attacks.

Impact Level Allocation

Low: SG.AT-2	Moderate: SG.AT-2	High: SG.AT-2

SG.AT-3 Security Training

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides security-related training—

1. Before authorizing access to the Smart Grid information system or performing assigned duties;
2. When required by Smart Grid information system changes; and
3. On an organization-defined frequency thereafter.

Supplemental Guidance

The organization determines the content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the Smart Grid information system to which personnel have authorized access. In addition, the organization provides Smart Grid information system managers, Smart Grid information system and network administrators,

and other personnel having access to Smart Grid information system-level software, security-related training to perform their assigned duties.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-3	Moderate: SG.AT-3	High: SG.AT-3

SG.AT-4 Security Awareness and Training Records

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization maintains a record of awareness and training for each user in accordance with the provisions of the organization's training and records retention policy.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-4	Moderate: SG.AT-4	High: SG.AT-4

SG.AT-5 Contact with Security Groups and Associations

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes and maintains contact with security groups and associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance

Security groups and associations can include special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.AT-6 Security Responsibility Testing

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the Smart Grid information system;
2. The organization maintains a list of security responsibilities for roles that are used to test each user in accordance with the provisions of the organization training policy; and
3. The security responsibility testing needs to be conducted on an organization-defined frequency and as warranted by technology/procedural changes.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-6	Moderate: SG.AT-6	High: SG.AT-6

SG.AT-7 Planning Process Training

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization includes training in the organization's planning process on the implementation of the Smart Grid information system security plans for employees, contractors, and third parties.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-7	Moderate: SG. AT-7	High: SG. AT-7

3.9 AUDIT AND ACCOUNTABILITY (SG.AU)

Periodic audits and logging of the Smart Grid information system need to be implemented to validate that the security mechanisms present during Smart Grid information system validation testing are still installed and operating correctly. These security audits review and examine a Smart Grid information system's records and activities to determine the adequacy of Smart Grid information system security requirements and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of Smart Grid information system logs. Logging is necessary for anomaly detection as well as forensic analysis.

SG.AU-1 Audit and Accountability Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented audit and accountability security policy that addresses—
      i. The objectives, roles, and responsibilities for the audit and accountability security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the audit and accountability security program as it applies to all of the organizational staff, contractors, and third parties.
   b. Procedures to address the implementation of the audit and accountability security policy and associated audit and accountability protection requirements.
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the audit and accountability security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The audit and accountability policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-1	Moderate: SG.AU-1	High: SG.AU-1

SG.AU-2 Auditable Events

Category: Common Technical Requirements, Integrity

Requirement

The organization—

1. Develops, based on a risk assessment, the Smart Grid information system list of auditable events on an organization-defined frequency;
2. Includes execution of privileged functions in the list of events to be audited by the Smart Grid information system; and
3. Revises the list of auditable events based on current threat data, assessment of risk, and post-incident analysis.

Supplemental Guidance

The purpose of this requirement is for the organization to identify events that need to be auditable as significant and relevant to the security of the Smart Grid information system.

Requirement Enhancements

1. The organization should audit activities associated with configuration changes to the Smart Grid information system.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-2	Moderate: SG.AU-2 (1)	High: SG.AU-2 (1)

SG.AU-3 Content of Audit Records

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system produces audit records for each event. The record contains the following information:

- Data and time of the event,
- The component of the Smart Grid information system where the event occurred,
- Type of event,
- User/subject identity, and
- The outcome of the events.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject; and

A2. The Smart Grid information system provides the capability to centrally manage the content of audit records generated by individual components throughout the Smart Grid information system.

Impact Level Allocation

Low: SG.AU-3	Moderate: SG.AU-3	High: SG.AU-3

SG.AU-4 Audit Storage Capacity

Category: Common Technical Requirements, Integrity

Requirement

The organization allocates organization-defined audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance

The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-4	Moderate: SG.AU-4	High: SG.AU-4

SG.AU-5 Response to Audit Processing Failures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system—

1. Alerts designated organizational officials in the event of an audit processing failure; and
2. Executes an organization-defined set of actions to be taken (e.g., shutdown Smart Grid information system, overwrite oldest audit records, and stop generating audit records).

Supplemental Guidance

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Requirement Enhancements

1. The Smart Grid information system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity; and
2. The Smart Grid information system provides a real-time alert for organization defined audit failure events.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-5	Moderate: SG.AU-5	High: SG.AU-5 (1), (2)

SG.AU-6 Audit Monitoring, Analysis, and Reporting

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Reviews and analyzes Smart Grid information system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to management authority; and
2. Adjusts the level of audit review, analysis, and reporting within the Smart Grid information system when a change in risk occurs to organizational operations, organizational assets, or individuals.

Supplemental Guidance

Organizations increase the level of audit monitoring and analysis activity within the Smart Grid information system based on, for example, law enforcement information, intelligence information, or other credible sources of information.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities;

A2. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness;

A3. The Smart Grid information system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the Smart Grid information system; and

A4. The organization integrates analysis of audit records with analysis of performance and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

Impact Level Allocation

Low: SG.AU-6	Moderate: SG.AU-6	High: SG.AU-6

SG.AU-7 Audit Reduction and Report Generation

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system provides an audit reduction and report generation capability.

Supplemental Guidance

Audit reduction and reporting may support near real-time analysis and after-the-fact investigations of security incidents.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system provides the capability to automatically process audit records for events of interest based on selectable event criteria

Impact Level Allocation

Low: Not Selected	Moderate: SG.AU-7	High: SG.AU-7

SG.AU-8 Time Stamps

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance

Time stamps generated by the information system include both date and time, as defined by the organization.

Requirement Enhancements

1. The Smart Grid information system synchronizes internal Smart Grid information system clocks on an organization-defined frequency using an organization-defined time source.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-8	Moderate: SG.AU-8 (1)	High: SG.AU-8 (1)

SG.AU-9 Protection of Audit Information

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance

Audit information includes, for example, audit records, audit settings, and audit reports.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system produces audit records on hardware-enforced, write-once media.

Impact Level Allocation

Low: SG.AU-9	Moderate: SG.AU-9	High: SG.AU-9

SG.AU-10 Audit Record Retention

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization retains audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-10	Moderate: SG.AU-10	High: SG.AU-10

SG.AU-11 Conduct and Frequency of Audits

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization conducts audits on an organization-defined frequency to assess conformance to specified security requirements and applicable laws and regulations.

Supplemental Guidance

Audits can be either in the form of internal self-assessment (sometimes called first-party audits) or independent, third-party audits.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-11	Moderate: SG.AU-11	High: SG.AU-11

SG.AU-12 Auditor Qualification

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization's audit program specifies auditor qualifications.

Supplemental Guidance

Security auditors need to—

1. Understand the Smart Grid information system and the associated operating practices;
2. Understand the risk involved with the audit; and
3. Understand the organization cyber security and the Smart Grid information system policy and procedures.

Requirement Enhancements

None.

Additional Considerations

A1. The organization assigns auditor and Smart Grid information system administration functions to separate personnel.

Impact Level Allocation

Low: SG.AU-12	Moderate: SG.AU-12	High: SG.AU-12

SG.AU-13 Audit Tools

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization specifies the rules and conditions of use of audit tools.

Supplemental Guidance

Access to Smart Grid information systems audit tools needs to be protected to prevent any possible misuse or compromise.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-13	Moderate: SG.AU-13	High: SG.AU-13

SG.AU-14 Security Policy Compliance

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program.

Supplemental Guidance

Periodic audits of the Smart Grid information system are implemented to demonstrate compliance to the organization's security policy. These audits—

1. Assess whether the defined cyber security policies and procedures, including those to identify security incidents, are being implemented and followed;
2. Document and ensure compliance to organization policies and procedures;
3. Identify security concerns, validate that the Smart Grid information system is free from security compromises, and provide information on the nature and extent of compromises should they occur;
4. Validate change management procedures and ensure that they produce an audit trail of reviews and approvals of all changes;
5. Verify that security mechanisms and management practices present during Smart Grid information system validation are still in place and functioning;
6. Ensure reliability and availability of the Smart Grid information system to support safe operation; and
7. Continuously improve performance.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-14	Moderate: SG.AU-14	High: SG.AU-14

SG.AU-15 Audit Generation

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system—

1. Provides audit record generation capability and generates audit records for the selected list of auditable events; and
2. Provides audit record generation capability and allows authorized users to select auditable events at the organization-defined Smart Grid information system components.

Supplemental Guidance

Audit records can be generated from various components within the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system provides the capability to compile audit records from multiple components within the Smart Grid information system into a Smart Grid information system-wide audit trail that is time-correlated to within an organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.

Impact Level Allocation

Low: SG.AU-15	Moderate: SG.AU-15	High: SG.AU-15

SG.AU-16 Non-Repudiation

Category: Unique Technical Requirements

Requirement

The Smart Grid information system protects against an individual falsely denying having performed a particular action.

Supplemental Guidance

Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services are implemented using various techniques (e.g., digital signatures, digital message receipts, and logging).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: SG.AU-16

3.10 SECURITY ASSESSMENT AND AUTHORIZATION (SG.CA)

Security assessments include monitoring and reviewing the performance of Smart Grid information system. Internal checking methods, such as compliance audits and incident investigations, allow the organization to determine the effectiveness of the security program. Finally, through continuous monitoring, the organization regularly reviews compliance of the Smart Grid information systems. If deviations or nonconformance exist, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.

SG.CA-1 Security Assessment and Authorization Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented security assessment and authorization policy that addresses—
      i. The objectives, roles, and responsibilities for the security assessment and authorization security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the security assessment and authorization security program as it applies to all of the organizational staff and third-party contractors; and
   b. Procedures to address the implementation of the security assessment and authorization policy and associated security assessment and authorization protection requirements;
2. Management commitment ensures compliance with the organization's security assessment and authorization security policy and other regulatory requirements; and
3. The organization ensures that the security assessment and authorization security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The authorization to operate and security assessment policies can be included as part of the general information security policy for the organization. Authorization to operate and security assessment procedures can be developed for the security program in general and for a particular Smart Grid information system when required. The organization defines significant change to a Smart Grid information system for security reauthorizations.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CA-1	Moderate: SG.CA-1	High: SG.CA-1

SG.CA-2 Security Assessments

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Develops a security assessment plan that describes the scope of the assessment including—
   a. Security requirements and requirement enhancements under assessment;
   b. Assessment procedures to be used to determine security requirement effectiveness; and
   c. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security requirements assessment to a management authority.

Supplemental Guidance

The organization assesses the security requirements in a Smart Grid information system as part of authorization or reauthorization to operate and continuous monitoring. Previous security assessment results may be reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs an independent assessor or assessment team to conduct an assessment of the security requirements in the Smart Grid information system.

Impact Level Allocation

Low: SG.CA-2	Moderate: SG.CA-2	High: SG.CA-2

SG.CA-3 Continuous Improvement

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization's security program implements continuous improvement practices to ensure that industry lessons learned and best practices are incorporated into Smart Grid information system security policies and procedures.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.CA-4 Smart Grid Information System Connections

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Authorizes all connections from the Smart Grid information system to other information systems;
2. Documents the Smart Grid information system connections and associated security requirements for each connection; and
3. Monitors the Smart Grid information system connections on an ongoing basis, verifying enforcement of documented security requirements.

Supplemental Guidance

The organization considers the risk that may be introduced when a Smart Grid information system is connected to other information systems, both internal and external to the organization, with different security requirements. Risk considerations also include Smart Grid information systems sharing the same networks.

Requirement Enhancements

None.

Additional Considerations

A1. All external Smart Grid information system and communication connections are identified and protected from tampering or damage.

Impact Level Allocation

Low: SG.CA-4	Moderate: SG.CA-4	High: SG.CA-4

SG.CA-5 Security Authorization to Operate

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization authorizes the Smart Grid information system for processing before operation and updates the authorization based on an organization-defined frequency or when a significant change occurs to the Smart Grid information system; and
2. A management authority signs and approves the security authorization to operate. Security assessments conducted in support of security authorizations need to be reviewed on an organization-defined frequency.

Supplemental Guidance

The organization assesses the security mechanisms implemented within the Smart Grid information system prior to security authorization to operate.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CA-5	Moderate: SG.CA-5	High: SG.CA-5

SG.CA-6 Continuous Monitoring

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy; and
2. Reporting the security state of the Smart Grid information system to management authority on an organization-defined frequency.

Supplemental Guidance

A continuous monitoring program allows an organization to maintain the security authorization to operate of a Smart Grid information system over time in a dynamic operational environment with changing threats, vulnerabilities, technologies, and missions/business processes.

The selection of an appropriate subset of security requirements for continuous monitoring is based on the impact level of the Smart Grid information system, the specific security requirements selected by the organization, and the level of assurance that the organization requires.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs an independent assessor or assessment team to monitor the security requirements in the Smart Grid information system on an ongoing basis;

A2. The organization includes as part of security requirements continuous monitoring, periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises; and

A3. The organization uses automated support tools for continuous monitoring.

Impact Level Allocation

Low: SG.CA-6	Moderate: SG.CA-6	High: SG.CA-6

3.11 CONFIGURATION MANAGEMENT (SG.CM)

The organization's security program needs to implement policies and procedures that create a process by which the organization manages and documents all configuration changes to the Smart Grid information system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the Smart Grid information system configuration. Smart Grid information systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a Smart Grid information system. Vendor updates and patches need to be thoroughly tested on a non-production Smart Grid information system setup before being introduced into the production environment to ensure that no adverse effects occur.

SG.CM-1 Configuration Management Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented configuration management security policy that addresses—
      i. The objectives, roles, and responsibilities for the configuration management security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the configuration management security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the configuration management security policy and associated configuration management protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and

3. The organization ensures that the configuration management security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The configuration management policy can be included as part of the general system security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-1	Moderate: SG.CM-1	High: SG.CM-1

SG.CM-2 Baseline Configuration

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops, documents, and maintains a current baseline configuration of the Smart Grid information system and an inventory of the Smart Grid information system's constituent components. The organization reviews and updates the baseline configuration as an integral part of Smart Grid information system component installations.

Supplemental Guidance

Maintaining the baseline configuration involves updating the baseline as the Smart Grid information system changes over time and keeping previous baselines for possible rollback.

Requirement Enhancements

None.

Additional Considerations

A1. The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration; and

A2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the Smart Grid information system.

Impact Level Allocation

Low: SG.CM-2	Moderate: SG.CM-2	High: SG.CM-2

SG.CM-3 Configuration Change Control

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Authorizes and documents changes to the Smart Grid information system;
2. Retains and reviews records of configuration-managed changes to the Smart Grid information system;
3. Audits activities associated with configuration-managed changes to the Smart Grid information system; and
4. Tests, validates, and documents configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system.

Supplemental Guidance

Configuration change control includes changes to the configuration settings for the Smart Grid information system and those IT products (e.g., operating systems, firewalls, routers) that are components of the Smart Grid information system. The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CM-3	High: SG.CM-3

SG.CM-4 Monitoring Configuration Changes

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization implements a process to monitor changes to the Smart Grid information system;
2. Prior to change implementation and as part of the change approval process, the organization analyzes changes to the Smart Grid information system for potential security impacts; and
3. After the Smart Grid information system is changed, the organization checks the security features to ensure that the features are still functioning properly.

Supplemental Guidance

Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional safeguards and countermeasures are required. The organization considers Smart Grid information system safety and security interdependencies.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-4	Moderate: SG.CM-4	High: SG.CM-4

SG.CM-5 Access Restrictions for Configuration Change

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Defines, documents, and approves individual access privileges and enforces access restrictions associated with configuration changes to the Smart Grid information system;
2. Generates, retains, and reviews records reflecting all such changes;
3. Establishes terms and conditions for installing any hardware, firmware, or software on Smart Grid information system devices; and
4. Conducts audits of Smart Grid information system changes at an organization-defined frequency and if/when suspected unauthorized changes have occurred.

Supplemental Guidance

Planned or unplanned changes to the hardware, software, and/or firmware components of the Smart Grid information system may affect the overall security of the Smart Grid information system. Only authorized individuals should be allowed to obtain access to Smart Grid information system components for purposes of initiating changes, including upgrades, and modifications. Maintaining records is important for supporting after-the-fact actions should the organization become aware of an unauthorized change to the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CM-5	High: SG.CM-5

SG.CM-6 Configuration Settings

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Establishes configuration settings for components within the Smart Grid information system;
2. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures;
3. Documents changed configuration settings;
4. Identifies, documents, and approves exceptions from the configuration settings; and
5. Enforces the configuration settings in all components of the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings;

A2. The organization employs automated mechanisms to respond to unauthorized changes to configuration settings; and

A3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

Impact Level Allocation

Low: SG.CM-6	Moderate: SG.CM-6	High: SG.CM-6

SG.CM-7 Configuration for Least Functionality

Category: Common Technical Requirements, Integrity

Requirement

1. The organization configures the Smart Grid information system to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally generated "prohibited and/or restricted" list; and
2. The organization reviews the Smart Grid information system on an organization-defined frequency or as deemed necessary to identify and restrict unnecessary functions, ports, protocols, and/or services.

Supplemental Guidance

The organization considers disabling unused or unnecessary physical and logical ports on Smart Grid information system components to prevent unauthorized connection of devices, and considers designing the overall system to enforce a policy of least functionality.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-7	Moderate: SG.CM-7	High: SG.CM-7

SG.CM-8 Component Inventory

Category: Common Technical Requirements, Integrity

Requirement

The organization develops, documents, and maintains an inventory of the components of the Smart Grid information system that—

1. Accurately reflects the current Smart Grid information system configuration;
2. Provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability;
3. Identifies the roles responsible for component inventory;
4. Updates the inventory of system components as an integral part of component installations, system updates, and removals; and
5. Ensures that the location (logical and physical) of each component is included within the Smart Grid information system boundary.

Supplemental Guidance

The organization determines the appropriate level of granularity for any Smart Grid information system component included in the inventory that is subject to management control (e.g., tracking, reporting).

Requirement Enhancements

None.

Additional Considerations

A1. The organization updates the inventory of the information system components as an integral part of component installations and information system updates;

A2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components; and

A3. The organization employs automated mechanisms to detect the addition of unauthorized components or devise into the environment and disables access by components or devices or notifies designated officials.

Impact Level Allocation

Low: SG.CM-8	Moderate: SG.CM-8	High: SG.CM-8

SG.CM-9 Addition, Removal, and Disposal of Equipment

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization implements policy and procedures to address the addition, removal, and disposal of all Smart Grid information system equipment; and
2. All Smart Grid information system components and information are documented, identified, and tracked so that their location and function are known.

Supplemental Guidance

The policies and procedures should consider the sensitivity of critical security parameters such as passwords, cryptographic keys, and personally identifiable information such as name and social security numbers.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-9	Moderate: SG.CM-9	High: SG.CM-9

SG.CM-10 Factory Default Settings Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization policy and procedures require the management of all factory default settings (e.g., authentication credentials, user names, configuration settings, and configuration parameters) on Smart Grid information system components and applications; and
2. The factory default settings should be changed upon installation and if used during maintenance.

Supplemental Guidance

Many Smart Grid information system devices and software are shipped with factory default settings to allow for initial installation and configuration.

Requirement Enhancements

None.

Additional Considerations

A1. The organization replaces default usernames whenever possible; and

A2. Default passwords of applications, operating systems, database management systems, or other programs must be changed within an organizational-defined time period.

Impact Level Allocation

Low: SG.CM-10	Moderate: SG.CM-10	High: SG.CM-10

SG.CM-11 Configuration Management Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops and implements a configuration management plan for the Smart Grid information system that—

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Defines the configuration items for the Smart Grid information system;
3. Defines when (in the system development life cycle) the configuration items are placed under configuration management;
4. Defines the means for uniquely identifying configuration items throughout the system development life cycle; and
5. Defines the process for managing the configuration of the controlled items.

Supplemental Guidance

The configuration management plan defines processes and procedures for how configuration management is used to support system development life cycle activities.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-11	Moderate: SG.CM-11	High: SG.CM-11

3.12 CONTINUITY OF OPERATIONS (SG.CP)

Continuity of operations addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal system operation. The ability for the Smart Grid information system to function after an event is dependent on implementing continuity of operations policies, procedures, training, and resources. The security requirements recommended under the continuity of operations family provide policies and procedures for roles and responsibilities, training, testing, plan updates, alternate storage sites, alternate command and control methods, alternate control centers, recovery and reconstitution and fail-safe response.

SG.CP-1 Continuity of Operations Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented continuity of operations security policy that addresses—
      i. The objectives, roles, and responsibilities for the continuity of operations security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the continuity of operations security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the continuity of operations security policy and associated continuity of operations protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the continuity of operations security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The continuity of operations policy can be included as part of the general information security policy for the organization. Continuity of operations procedures can be developed for the security program in general, and for a particular Smart Grid information system, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-1	Moderate: SG.CP-1	High: SG.CP-1

SG.CP-2 Continuity of Operations Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system;
2. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring Smart Grid information system operations after a disruption or failure; and
3. A management authority reviews and approves the continuity of operations plan.

Supplemental Guidance

A continuity of operations plan addresses both business continuity planning and recovery of Smart Grid information system operations. Development of a continuity of operations plan is a process to identify procedures for safe Smart Grid information system operation while recovering from a Smart Grid information system disruption. The plan requires documentation of critical Smart Grid information system functions that need to be recovered.

Requirement Enhancements

None.

Additional Considerations

A1. The organization performs a root cause analysis for the event and submits any findings from the analysis to management.

Impact Level Allocation

Low: SG.CP-2	Moderate: SG.CP-2	High: SG.CP-2

SG.CP-3 Continuity of Operations Roles and Responsibilities

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The continuity of operations plan—

1. Defines the roles and responsibilities of the various employees and contractors in the event of a significant incident; and
2. Identifies responsible personnel to lead the recovery and response effort if an incident occurs.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-3	Moderate: SG.CP-3	High: SG.CP-3

SG.CP-4 Continuity of Operations Training

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization trains personnel in their continuity of operations roles and responsibilities with respect to the Smart Grid information system and provides refresher training on an organization-defined frequency.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-4	Moderate: SG.CP-4	High: SG.CP-4

SG.CP-5 Continuity of Operations Plan Testing

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The continuity of operations plan is tested to determine its effectiveness and results are documented;
2. A management authority reviews the documented test results and initiates corrective actions, if necessary; and
3. The organization tests the continuity of operations plan for the Smart Grid information system on an organization-defined frequency, using defined tests.

Supplemental Guidance

None.

Requirement Enhancements

1. The organization coordinates continuity of operations plan testing and exercises with all affected organizational elements.

Additional Considerations

A1. The organization employs automated mechanisms to test/exercise the continuity of operations plan; and

A2. The organization tests/exercises the continuity of operations plan at the alternate processing site to familiarize Smart Grid information system operations personnel with the facility and available resources and to evaluate the site's capabilities to support continuity of operations.

Impact Level Allocation

Low: SG.CP-5	Moderate: SG. CP-5 (1)	High: SG. CP-5 (1)

SG.CP-6 Continuity of Operations Plan Update

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization reviews the continuity of operations plan for the Smart Grid information system and updates the plan to address Smart Grid information system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing on an organization-defined frequency.

Supplemental Guidance

Organizational changes include changes in mission, functions, or business processes supported by the Smart Grid information system. The organization communicates the changes to appropriate organizational elements.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-6	Moderate: SG.CP-6	High: SG.CP-6

SG.CP-7 Alternate Storage Sites

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization determines the requirement for an alternate storage site and initiates any necessary agreements.

Supplemental Guidance

The Smart Grid information system backups and the transfer rate of backup information to the alternate storage site are performed on an organization-defined frequency.

Requirement Enhancements

1. The organization identifies potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions;
2. The organization identifies an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards; and
3. The organization configures the alternate storage site to facilitate timely and effective recovery operations.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CP-7 (1), (2)	High: SG.SG.CP-7 (1), (2), (3)

SG.CP-8 Alternate Telecommunication Services

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization identifies alternate telecommunication services for the Smart Grid information system and initiates necessary agreements to permit the resumption of operations for the safe operation of the Smart Grid information system within an organization-defined time period when the primary Smart Grid information system capabilities are unavailable.

Supplemental Guidance

Alternate telecommunication services required to resume operations within the organization-defined time period are either available at alternate organization sites or contracts with vendors need to be in place to support alternate telecommunication services for the Smart Grid information system.

Requirement Enhancements

1. Primary and alternate telecommunication service agreements contain priority-of-service provisions in accordance with the organization's availability requirements;
2. Alternate telecommunication services do not share a single point of failure with primary telecommunication services;
3. Alternate telecommunication service providers need to be sufficiently separated from primary service providers so they are not susceptible to the same hazards; and
4. Primary and alternate telecommunication service providers need to have adequate contingency plans.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CP-8 (1), (4)	High: SG. CP-8 (1), (2), (3), (4)

SG.CP-9 Alternate Control Center

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization identifies an alternate control center, necessary telecommunications, and initiates any necessary agreements to permit the resumption of Smart Grid information system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable.

Supplemental Guidance

Equipment, telecommunications, and supplies required to resume operations within the organization-prescribed time period need to be available at the alternative control center or by a contract in place to support delivery to the site.

Requirement Enhancements

1. The organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards;
2. The organization identifies potential accessibility problems to the alternate control center in the event of an area-wide disruption or disaster and outlines explicit mitigation actions; and
3. The organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

Additional Considerations

A1. The organization fully configures the alternate control center and telecommunications so that they are ready to be used as the operational site supporting a minimum required operational capability; and

A2. The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CP-9 (1), (2), (3)	High: SG.CP-9 (1), (2), (3)

SG.CP-10 Smart Grid Information System Recovery and Reconstitution

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides the capability to recover and reconstitute the Smart Grid information system to a known secure state after a disruption, compromise, or failure.

Supplemental Guidance

Smart Grid information system recovery and reconstitution to a known secure state means that—

1. All Smart Grid information system parameters (either default or organization-established) are set to secure values;
2. Security-critical patches are reinstalled;
3. Security-related configuration settings are reestablished;
4. Smart Grid information system documentation and operating procedures are available;
5. Application and Smart Grid information system software is reinstalled and configured with secure settings;
6. Information from the most recent, known secure backups is loaded; and
7. The Smart Grid information system is fully tested.

Requirement Enhancements

1. The organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state; and
2. The organization provides the capability to reimage Smart Grid information system components in accordance with organization-defined restoration time periods from configuration-controlled and integrity-protected media images representing a secure, operational state for the components.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-10	Moderate: SG.CP-10 (1)	High: SG.CP-10 (1), (2)

SG.CP-11 Fail-Safe Response

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other Smart Grid information systems or the loss of the Smart Grid information system itself.

Supplemental Guidance

In the event of a loss of communication between the Smart Grid information system and the operational facilities, the on-site instrumentation needs to be capable of executing a procedure that provides the maximum protection to the controlled infrastructure. For the electric sector, this may be to alert the operator of the failure and then do nothing (i.e., let the electric grid continue to operate). The organization defines what "loss of communications" means (e.g., 5 seconds or 5 minutes without communications). The organization then defines the appropriate fail-safe process for its industry.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system preserves the organization-defined state information in failure.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: SG.CP-11

3.13 IDENTIFICATION AND AUTHENTICATION (SG.IA)

Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a Smart Grid information system.

SG.IA-1 Identification and Authentication Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented identification and authentication security policy that addresses—
      i. The objectives, roles, and responsibilities for the identification and authentication security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the identification and authentication security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the identification and authentication security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The identification and authentication policy can be included as part of the general security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IA-1	Moderate: SG.IA-1	High: SG.IA-1

SG.IA-2 Identifier Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization receives authorization from a management authority to assign a user or device identifier.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization archives previous user or device identifiers; and

A2. The organization selects an identifier that uniquely identifies an individual or device.

Impact Level Allocation

Low: SG.IA-2	Moderate: SG.IA-2	High: SG.IA-2

SG.IA-3 Authenticator Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization manages Smart Grid information system authentication credentials for users and devices by—

1. Defining initial authentication credential content, such as defining password length and composition, tokens;
2. Establishing administrative procedures for initial authentication credential distribution; lost, compromised, or damaged authentication credentials; and revoking authentication credentials;
3. Changing/refreshing authentication credentials on an organization-defined frequency; and
4. Specifying measures to safeguard authentication credentials.

Supplemental Guidance

Measures to safeguard user authentication credentials include maintaining possession of individual authentication credentials, not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated tools to determine if authentication credentials are sufficiently strong to resist attacks intended to discover or otherwise compromise the authentication credentials; and

A2. The organization requires unique authentication credentials be provided by vendors and manufacturers of Smart Grid information system components.

Impact Level Allocation

Low: SG.IA-3	Moderate: SG.IA-3	High: SG.IA-3

SG.IA-4 User Identification and Authentication

Category: Unique Technical Requirements

Requirement

The Smart Grid information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system uses multifactor authentication for—

a. Remote access to non-privileged accounts;

b. Local access to privileged accounts; and

c. Remote access to privileged accounts.

Impact Level Allocation

Low: SG.IA-4	Moderate: SG.IA-4	High: SG.IA-4

SG.IA-5 Device Identification and Authentication

Category: Unique Technical Requirements

Requirement

The Smart Grid information system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection.

Supplemental Guidance

The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization.

Requirement Enhancements

1. The Smart Grid information system authenticates devices before establishing remote network connections using bidirectional authentication between devices that is cryptographically based; and
2. The Smart Grid information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.IA-5 (1), (2)	High: SG.IA-5 (1), (2)

SG.IA-6 Authenticator Feedback

Category: Unique Technical Requirements

Requirement

The authentication mechanisms in the Smart Grid information system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance

The Smart Grid information system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the Smart Grid information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IA-6	Moderate: SG.IA-6	High: SG.IA-6

3.14 INFORMATION AND DOCUMENT MANAGEMENT (SG.ID)

Information and document management is generally a part of the organization records retention and document management system. Digital and hardcopy information associated with the development and execution of a Smart Grid information system is important and sensitive, and need to be managed. Smart Grid information system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive organization information and need to be protected. This information must be protected and verified that the appropriate versions are retained.

The following are the requirements for Information and Document Management that need to be supported and implemented by the organization to protect the Smart Grid information system.

SG.ID-1 Information and Document Management Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A Smart Grid information and document management policy that addresses—

i. The objectives, roles and responsibilities for the information and document management security program as it relates to protecting the organization's personnel and assets;

ii. The scope of the information and document management security program as it applies to all the organizational staff, contractors, and third parties;

iii. The retrieval of written and electronic records, equipment, and other media for the Smart Grid information system; and

iv. The destruction of written and electronic records, equipment, and other media for the Smart Grid information system; and

b. Procedures to address the implementation of the information and document management security policy and associated Smart Grid information system information and document management protection requirements;

2. Management commitment ensures compliance of the organization's security policy and other regulatory requirements; and

3. The organization ensures that the Smart Grid information system information and document management policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The information and document management policy may be included as part of the general information security policy for the organization. The information and document management procedures can be developed for the security program in general and for a particular Smart Grid information system when required. The organization employs appropriate measures to ensure that long-term records and information can be retrieved (e.g., converting the data to a newer format, retaining older equipment that can read the data). Destruction includes the method of disposal such as shredding of paper records, erasing of disks or other electronic media, or physical destruction.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.ID-1	Moderate: SG.ID-1	High: SG.ID-1

SG.ID-2 Information and Document Retention

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops policies and procedures detailing the retention of organization information;

2. The organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations;
3. The organization manages Smart Grid information system-related data including establishing retention policies and procedures for both electronic and paper data; and
4. The organization manages access to Smart Grid information system-related data based on assigned roles and responsibilities.

Supplemental Guidance

The retention procedures address retention/destruction issues for all applicable information media.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.ID-2	Moderate: SG.ID-2	High: SG.ID-2

SG.ID-3 Information Handling

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

Organization-implemented policies and procedures detailing the handling of information are developed and reviewed on an organization-defined frequency.

Supplemental Guidance

Written policies and procedures detail access, sharing, copying, transmittal, distribution, and disposal or destruction of Smart Grid information system information. These policies or procedures include the periodic review of all information to ensure that it is properly handled.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.ID-3	Moderate: SG.ID-3	High: SG.ID-3

SG.ID-4 Information Exchange

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

Agreements are established for the exchange of information, firmware, and software between the organization and external parties such as third parties, vendors and contractors.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. If a specific device needs to communicate with another device outside the Smart Grid information system, communications need to be limited to only the devices that need to communicate.

Impact Level Allocation

Low: SG.ID-4	Moderate: SG.ID-4	High: SG.ID-4

SG.ID-5 Automated Labeling

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system automatically labels information in storage, in process, and in transmission in accordance with—

1. Access control requirements;
2. Special dissemination, handling, or distribution instructions; and
3. Otherwise as required by the Smart Grid information system security policy.

Supplemental Guidance

Automated labeling refers to labels employed on internal data structures (e.g., records, buffers, files) within the Smart Grid information system. Such labels are often used to implement access control and flow control policies.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system maintains the binding of the label to the information.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

3.15 INCIDENT RESPONSE (SG.IR)

Incident response addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal Smart Grid information system operation. Incident response entails the preparation, testing, and maintenance of specific policies

and procedures to enable the organization to recover the Smart Grid information system's operational status after the occurrence of a disruption. Disruptions can come from natural disasters, such as earthquakes, tornados, floods, or from manmade events like riots, terrorism, or vandalism. The ability for the Smart Grid information system to function after such an event is directly dependent on implementing policies, procedures, training, and resources in place ahead of time using the organization's planning process. The security requirements recommended under the incident response family provide policies and procedures for incident response monitoring, handling, reporting, testing, training, recovery, and reconstitution of the Smart Grid information systems for an organization.

SG.IR-1 Incident Response Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
    a. A documented incident response security policy that addresses—
        i. The objectives, roles, and responsibilities for the incident response security program as it relates to protecting the organization's personnel and assets; and
        ii. The scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties; and
    b. Procedures to address the implementation of the incident response security policy and associated incident response protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements;
3. The organization ensures that the incident response security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations; and
4. The organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood."

Supplemental Guidance

The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular Smart Grid information system, when required. The various types of incidents that may result from system intrusion need to be identified and classified as to their effects and likelihood so that a proper response can be formulated for each potential incident. The organization determines the impact to each Smart Grid system and the consequences associated with loss of one or more of the Smart Grid information systems.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-1	Moderate: SG.IR-1	High: SG.IR-1

SG.IR-2 Incident Response Roles and Responsibilities

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization's Smart Grid information system security plan defines the specific roles and responsibilities in relation to various types of incidents; and
2. The plan identifies responsible personnel to lead the response effort if an incident occurs. Response teams need to be formed, including Smart Grid information system and other process owners, to reestablish operations.

Supplemental Guidance

The organization's Smart Grid information system security plan defines the roles and responsibilities of the various employees, contractors, and third parties in the event of an incident. The response teams have a major role in the interruption identification and planning process.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-2	Moderate: SG.IR-2	High: SG.IR-2

SG.IR-3 Incident Response Training

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

Personnel are trained in their incident response roles and responsibilities with respect to the Smart Grid information system and receive refresher training on an organization-defined frequency.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization incorporates Smart Grid information system simulated events into continuity of operations training to facilitate effective response by personnel in crisis situations; and

A2. The organization employs automated mechanisms to provide a realistic Smart Grid information system training environment.

Impact Level Allocation

Low: SG.IR-3	Moderate: SG.IR-3	High: SG.IR-3

SG.IR-4 Incident Response Testing and Exercises

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization tests and/or exercises the incident response capability for the information system at an organization-defined frequency using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability

Impact Level Allocation

Low: SG.IR-4	Moderate: SG.IR-4	High: SG.IR-4

SG.IR-5 Incident Handling

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, mitigation, and recovery;
2. Integrates incident handling procedures with continuity of operations procedures; and
3. Incorporates lessons learned from incident handling activities into incident response procedures.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to administer and support the incident handling process.

Impact Level Allocation

Low: SG.IR-5	Moderate: SG.IR-5	High: SG.IR-5

SG.IR-6 Incident Monitoring

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization tracks and documents Smart Grid information system and network security incidents.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Impact Level Allocation

Low: SG.IR-6	Moderate: SG.IR-6	High: SG.IR-6

SG.IR-7 Incident Reporting

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization incident reporting procedure includes:
   a. What is a reportable incident;
   b. The granularity of the information reported;
   c. Who receives the report; and
   d. The process for transmitting the incident information.
2. Detailed incident data is reported in a manner that complies with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to assist in the reporting of security incidents.

Impact Level Allocation

Low: SG.IR-7	Moderate: SG.IR-7	High: SG.IR-7

SG.IR-8 Incident Response Investigation and Analysis

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization policies and procedures include an incident response investigation and analysis program;
2. The organization includes investigation and analysis of Smart Grid information system incidents in the planning process; and
3. The organization develops, tests, deploys, and documents an incident investigation and analysis process.

Supplemental Guidance

The organization documents its policies and procedures to show that investigation and analysis of incidents are included in the planning process. The procedures ensure that the Smart Grid information system is capable of providing event data to the proper personnel for analysis and for developing mitigation steps.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-8	Moderate: SG.IR-8	High: SG.IR-8

SG.IR-9 Corrective Action

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization reviews investigation results and determines corrective actions needed; and
2. The organization includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of cyber security and Smart Grid information system incidents are fully implemented.

Supplemental Guidance

The organization encourages and promotes cross-industry incident information exchange and cooperation to learn from the experiences of others.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-9	Moderate: SG.IR-9	High: SG.IR-9

SG.IR-10 Smart Grid Information System Backup

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Conducts backups of user-level information contained in the Smart Grid information system on an organization-defined frequency;
2. Conducts backups of Smart Grid information system-level information (including Smart Grid information system state information) contained in the Smart Grid information system on an organization-defined frequency;
3. Conducts backups of information system documentation including security-related documentation on an organization-defined frequency consistent with recovery time; and
4. Protects the confidentiality and integrity of backup information at the storage location.

Supplemental Guidance

The protection of Smart Grid information system backup information while in transit is beyond the scope of this requirement.

Requirement Enhancements

1. The organization tests backup information at an organization-defined frequency to verify media reliability and information integrity;
2. The organization selectively uses backup information in the restoration of Smart Grid information system functions as part of continuity of operations testing; and
3. The organization stores backup copies of the operating system and other critical Smart Grid information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-10	Moderate: SG.IR-10 (1)	High: SG.IR-10 (1), (2), (3)

SG.IR-11 Coordination of Emergency Response

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization's security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.

Supplemental Guidance

The organization expands relationships with local emergency response personnel to include information sharing and coordinated response to cyber security incidents.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-11	Moderate: SG.IR-11	High: SG.IR-11

3.16 SMART GRID INFORMATION SYSTEM DEVELOPMENT AND MAINTENANCE (SG.MA)

Security is most effective when it is designed into the Smart Grid information system and sustained, through effective maintenance, throughout the life cycle of the Smart Grid information system. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a Smart Grid information system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.

SG.MA-1 Smart Grid Information System Maintenance Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
    a. A documented Smart Grid information system maintenance security policy that addresses—
        i. The objectives, roles, and responsibilities for the Smart Grid information system maintenance security program as it relates to protecting the organization's personnel and assets; and
        ii. The scope of the Smart Grid information system maintenance security program as it applies to all of the organizational staff, contractors, and third parties; and

b. Procedures to address the implementation of the Smart Grid information system maintenance security policy and associated Smart Grid information system maintenance protection requirements;

2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the Smart Grid information system maintenance security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The Smart Grid information system maintenance policy can be included as part of the general information security policy for the organization. Smart Grid information system maintenance procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MA-1	Moderate: SG.MA-1	High: SG.MA-1

SG.MA-2 Legacy Smart Grid Information System Upgrades

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops policies and procedures to upgrade existing legacy Smart Grid information systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MA-2	Moderate: SG.MA-2	High: SG.MA-2

SG.MA-3 Smart Grid Information System Maintenance

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Schedules, performs, documents, and reviews records of maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. Explicitly approves the removal of the Smart Grid information system or Smart Grid information system components from organizational facilities for off-site maintenance or repairs;
3. Sanitizes the equipment to remove all critical/sensitive information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
4. Checks all potentially impacted security requirements to verify that the requirements are still functioning properly following maintenance or repair actions; and
5. Makes and secures backups of critical Smart Grid information system software, applications, and data for use if the operating system becomes corrupted or destroyed.

Supplemental Guidance

All maintenance activities to include routine, scheduled maintenance and repairs, and unplanned maintenance are controlled whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Maintenance procedures that require the physical removal of any Smart Grid information system component needs to be documented, listing the date, time, reason for removal, estimated date of reinstallation, and name personnel removing components.

Requirement Enhancements

1. The organization maintains maintenance records for the Smart Grid information system that include:
   a. The date and time of maintenance;
   b. Name of the individual performing the maintenance;
   c. Name of escort, if necessary;
   d. A description of the maintenance performed; and
   e. A list of equipment removed or replaced (including identification numbers, if applicable).

Additional Considerations

A1. The organization employs automated mechanisms to schedule and document maintenance and repairs as required, producing up-to-date, accurate, complete, and available records of all maintenance and repair actions needed, in process, and completed.

Impact Level Allocation

Low: SG.MA-3	Moderate: SG.MA-3	High: SG.MA-3 (1)

SG.MA-4 Maintenance Tools

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization approves and monitors the use of Smart Grid information system maintenance tools.

Supplemental Guidance

The requirement addresses security-related issues when the hardware, firmware, and software are brought into the Smart Grid information system for diagnostic and repair actions.

Requirement Enhancements

None.

Additional Considerations

A1. The organization requires approval from a management authority explicitly authorizing removal of equipment from the facility;

A2. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications;

A3. The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the Smart Grid information system; and

A4. The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

Impact Level Allocation

Low: SG.MA-4	Moderate: SG.MA-4	High: SG.MA-4

SG.MA-5 Maintenance Personnel

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization documents authorization and approval policies and procedures for maintaining a list of personnel authorized to perform maintenance on the Smart Grid information system; and
2. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the Smart Grid information system.

Supplemental Guidance

Maintenance personnel need to have appropriate access authorization to the Smart Grid information system when maintenance activities allow access to organizational information that could result in a future compromise of availability, integrity, or confidentiality.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MA-5	Moderate: SG.MA-5	High: SG.MA-5

SG.MA-6 Remote Maintenance

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization policy and procedures for remote maintenance include:

1. Authorization and monitoring the use of remote maintenance and diagnostic activities;
2. Use of remote maintenance and diagnostic tools;
3. Maintenance records for remote maintenance and diagnostic activities;
4. Termination of all remote maintenance sessions; and
5. Management of authorization credentials used during remote maintenance.

Supplemental Guidance

None.

Requirement Enhancements

The organization—

1. Requires that remote maintenance or diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the Smart Grid information system being serviced; or
2. Removes the component to be serviced from the Smart Grid information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities and after the service is performed, sanitizes the component (with regard to potentially malicious software) before returning the component to the Smart Grid information system.

Additional Considerations

A1. The organization requires that remote maintenance sessions are protected through the use of a strong authentication credential; and

A2. The organization requires that (a) maintenance personnel notify the Smart Grid information system administrator when remote maintenance is planned (e.g., date/time), and (b) a management authority approves the remote maintenance.

Impact Level Allocation

Low: SG.MA-6	Moderate: SG.MA-6	High: SG.MA-6 (1)

SG.MA-7 Timely Maintenance

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization obtains maintenance support and spare parts for an organization-defined list of security-critical Smart Grid information system components.

Supplemental Guidance

The organization specifies those Smart Grid information system components that, when not operational, result in increased risk to organizations or individuals because the security functionality intended by that component is not being provided.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MA-7	Moderate: SG.MA-7	High: SG.MA-7

3.17 MEDIA PROTECTION (SG.MP)

The security requirements under the media protection family provide policy and procedures for limiting access to media to authorized users. Security measures also exist for distribution and handling requirements as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media. Media assets include compact discs; digital video discs; erasable, programmable read-only memory; tapes; printed reports; and documents.

SG.MP-1 Media Protection Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented media protection security policy that addresses—
      i. The objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the media protection security policy and associated media protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and

3. The organization ensures that the media protection security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The media protection policy can be included as part of the general security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MP-1	Moderate: SG.MP-1	High: SG.MP-1

SG.MP-2 Media Sensitivity Level

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The sensitivity level of media indicates the protection required commensurate with the impact of compromise.

Supplemental Guidance

These media sensitivity levels provide guidance for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MP-2	Moderate: SG.MP-2	High: SG.MP-2

SG.MP-3 Media Marking

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization marks removable Smart Grid information system media and Smart Grid information system output in accordance with organization-defined policy and procedures.

Supplemental Guidance

Smart Grid information system markings refer to the markings employed on external media (e.g., video displays, hardcopy documents output from the Smart Grid information system).

External markings are distinguished from internal markings (i.e., the labels used on internal data structures within the Smart Grid information system).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.MP-3	High: SG.MP-3

SG.MP-4 Media Storage

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization physically manages and stores Smart Grid information system media within protected areas. The sensitivity of the material determines how the media are stored.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MP-4	Moderate: SG.MP-4	High: SG.MP-4

SG.MP-5 Media Transport

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Protects organization-defined types of media during transport outside controlled areas using organization-defined security measures;
2. Maintains accountability for Smart Grid information system media during transport outside controlled areas; and
3. Restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance

A controlled area is any space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs an identified custodian throughout the transport of Smart Grid information system media; and

A2. The organization documents activities associated with the transport of Smart Grid information system media using an organization-defined Smart Grid information system of records.

Impact Level Allocation

Low: SG.MP-5	Moderate: SG.MP-5	High: SG.MP-5

SG.MP-6 Media Sanitization and Disposal

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization sanitizes Smart Grid information system media before disposal or release for reuse. The organization tests sanitization equipment and procedures to verify correct performance on an organization-defined frequency.

Supplemental Guidance

Sanitization is the process of removing information from media such that data recovery is not possible.

Requirement Enhancements

The organization tracks, documents, and verifies media sanitization and disposal actions.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MP-6	Moderate: SG.MP-6 (1)	High: SG.MP-6 (1)

3.18 PHYSICAL AND ENVIRONMENTAL SECURITY (SG.PE)

Physical and environmental security encompasses protection of physical assets from damage, misuse, or theft. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access Smart Grid information systems and components. Environmental security addresses the safety of assets from damage from environmental concerns. Physical and environmental security addresses protection from environmental threats.

SG.PE-1 Physical and Environmental Security Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented physical and environmental security policy that addresses—
      i. The objectives, roles, and responsibilities for the physical and environmental security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the physical and environmental security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the physical and environmental security policy and associated physical and environmental protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the physical and environmental security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The organization may include the physical and environmental security policy as part of the general security policy for the organization.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-1	Moderate: SG.PE-1	High: SG.PE-1

SG.PE-2 Physical Access Authorizations

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops and maintains lists of personnel with authorized access to facilities containing Smart Grid information systems and issues appropriate authorization credentials (e.g., badges, identification cards); and
2. Designated officials within the organization review and approve access lists on an organization-defined frequency, removing from the access lists personnel no longer requiring access.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization authorizes physical access to the facility where the Smart Grid information system resides based on position or role;

A2. The organization requires multiple forms of identification to gain access to the facility where the Smart Grid information system resides; and

A3. The organization requires multifactor authentication to gain access to the facility where the Smart Grid information system resides.

Impact Level Allocation

Low: SG.PE-2	Moderate: SG.PE-2	High: SG.PE-2

SG.PE-3 Physical Access

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Enforces physical access authorizations for all physical access points to the facility where the Smart Grid information system resides;
2. Verifies individual access authorizations before granting access to the facility;
3. Controls entry to facilities containing Smart Grid information systems;
4. Secures keys, combinations, and other physical access devices;
5. Inventories physical access devices on a periodic basis; and
6. Changes combinations, keys, and authorization credentials on an organization-defined frequency and when keys are lost, combinations are compromised, individual credentials are lost, or individuals are transferred or terminated.

Supplemental Guidance

Physical access devices include keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational Smart Grid information system may be located in areas designated as publicly accessible with access to such devices being safeguarded.

Requirement Enhancements

1. The organization requires physical access mechanisms to Smart Grid information system assets in addition to physical access mechanisms to the facility; and
2. The organization employs hardware to deter unauthorized physical access to Smart Grid information system devices.

Additional Considerations

A1. The organization ensures that every physical access point to the facility where the Smart Grid information system resides is guarded or alarmed and monitored on an organization-defined frequency.

Impact Level Allocation

Low: SG.PE-3	Moderate: SG.PE-3 (2)	High: SG.PE-3 (1), (2)

SG.PE-4 Monitoring Physical Access

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Monitors physical access to the Smart Grid information system to detect and respond to physical security incidents;
2. Reviews physical access logs on an organization-defined frequency;
3. Coordinates results of reviews and investigations with the organization's incident response capability; and
4. Ensures that investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization installs and monitors real-time physical intrusion alarms and surveillance equipment; and

A2. The organization implements automated mechanisms to recognize potential intrusions and initiates designated response actions.

Impact Level Allocation

Low: SG.PE-4	Moderate: SG.PE-4	High: SG.PE-4

SG.PE-5 Visitor Control

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization controls physical access to the Smart Grid information system by authenticating visitors before authorizing access to the facility.

Supplemental Guidance

Contractors and others with permanent authorization credentials are not considered visitors.

Requirement Enhancements

The organization escorts visitors and monitors visitor activity as required according to security policies and procedures.

Additional Considerations

A1. The organization requires multiple forms of identification for access to the facility.

Impact Level Allocation

Low: SG.PE-5	Moderate: SG.PE-5 (1)	High: SG.PE-5 (1)

SG.PE-6 Visitor Records

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization maintains visitor access records to the facility that include:

1. Name and organization of the person visiting;
2. Signature of the visitor;
3. Form of identification;
4. Date of access;
5. Time of entry and departure;
6. Purpose of visit; and
7. Name and organization of person visited.

Designated officials within the organization review the access logs after closeout and periodically review access logs based on an organization-defined frequency.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to facilitate the maintenance and review of access records.

Impact Level Allocation

Low: SG.PE-6	Moderate: SG.PE-6	High: SG.PE-6

SG.PE-7 Physical Access Log Retention

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-7	Moderate: SG.PE-7	High: SG.PE-7

SG.PE-8 Emergency Shutoff Protection

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization protects the emergency power-off capability from accidental and intentional/unauthorized activation.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-8	Moderate: SG.PE-8	High: SG.PE-8

SG.PE-9 Emergency Power

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides an alternate power supply to facilitate an orderly shutdown of noncritical Smart Grid information system components in the event of a primary power source loss.

Supplemental Guidance

None.

Requirement Enhancements

1. The organization provides a long-term alternate power supply for the Smart Grid information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Additional Considerations

A1. The organization provides a long-term alternate power supply for the Smart Grid information system that is self-contained and not reliant on external power generation.

Impact Level Allocation

Low: SG.PE-9	Moderate: SG.PE-9 (1)	High: SG.PE-9 (1)

SG.PE-10 Delivery and Removal

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization authorizes, monitors, and controls organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items.

Supplemental Guidance

The organization secures delivery areas and, if possible, isolates delivery areas from the Smart Grid information system to avoid unauthorized physical access.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-10	Moderate: SG.PE-10	High: SG.PE-10

SG.PE-11 Alternate Work Site

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization establishes an alternate work site (for example, private residences) with proper equipment and communication infrastructure to compensate for the loss of the primary work site; and
2. The organization implements appropriate management, operational, and technical security measures at alternate control centers.

Supplemental Guidance

The organization may define different sets of security requirements for specific alternate work sites or types of sites.

Requirement Enhancements

None.

Additional Considerations

A1. The organization provides methods for employees to communicate with Smart Grid information system security staff in case of security problems.

Impact Level Allocation

Low: SG.PE-11	Moderate: SG.PE-11	High: SG.PE-11

SG.PE-12 Location of Smart Grid Information System Assets

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization locates Smart Grid information system assets to minimize potential damage from physical and environmental hazards.

Supplemental Guidance

Physical and environmental hazards include flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation.

Requirement Enhancements

1. The organization considers the risk associated with physical and environmental hazards when planning new Smart Grid information system facilities or reviewing existing facilities.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-12	Moderate: SG.PE-12	High: SG.PE-12 (1)

3.19 PLANNING (SG.PL)

The purpose of strategic planning is to maintain optimal operations and to prevent or recover from undesirable interruptions to Smart Grid information system operation. Interruptions may take the form of a natural disaster (hurricane, tornado, earthquake, flood, etc.), an unintentional manmade event (accidental equipment damage, fire or explosion, operator error, etc.), an intentional manmade event (attack by bomb, firearm or vandalism, hacker or malware, etc.), or an equipment failure. The types of planning considered are security planning to prevent undesirable interruptions, continuity of operations planning to maintain Smart Grid information system operation during and after an interruption, and planning to identify mitigation strategies.

SG.PL-1 Strategic Planning Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented planning policy that addresses—
      i. The objectives, roles, and responsibilities for the planning program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the planning program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the planning policy and associated strategic planning requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the planning policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The strategic planning policy may be included as part of the general information security policy for the organization. Strategic planning procedures may be developed for the security program in general and a Smart Grid information system in particular, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PL-1	Moderate: SG.PL-1	High: SG.PL-1

SG.PL-2 Smart Grid Information System Security Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Develops a security plan for each Smart Grid information system that—
   a. Aligns with the organization's enterprise architecture;
   b. Explicitly defines the components of the Smart Grid information system;
   c. Describes relationships with and interconnections to other Smart Grid information systems;

d. Provides an overview of the security objectives for the Smart Grid information system;

e. Describes the security requirements in place or planned for meeting those requirements; and

f. Is reviewed and approved by the management authority prior to plan implementation;

2. Reviews the security plan for the Smart Grid information system on an organization-defined frequency; and

3. Revises the plan to address changes to the Smart Grid information system/environment of operation or problems identified during plan implementation or security requirement assessments.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PL-2	Moderate: SG.PL-2	High: SG.PL-2

SG.PL-3 Rules of Behavior

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes and makes readily available to all Smart Grid information system users, a set of rules that describes their responsibilities and expected behavior with regard to Smart Grid information system usage.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial Web sites, and sharing Smart Grid information system account information; and

A2. The organization obtains signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the Smart Grid information system.

Impact Level Allocation

Low: SG.PL-3	Moderate: SG.PL-3	High: SG.PL-3

SG.PL-4 Privacy Impact Assessment

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization conducts a privacy impact assessment on the Smart Grid information system; and
2. The privacy impact assessment is reviewed and approved by a management authority.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PL-4	Moderate: SG.PL-4	High: SG.PL-4

SG.PL-5 Security-Related Activity Planning

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization plans and coordinates security-related activities affecting the Smart Grid information system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals; and
2. Organizational planning and coordination includes both emergency and nonemergency (e.g., routine) situations.

Supplemental Guidance

Routine security-related activities include, but are not limited to, security assessments, audits, Smart Grid information system hardware, firmware, and software maintenance, and testing/exercises.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.PL-5	High: SG.PL-5

3.20 SECURITY PROGRAM MANAGEMENT (SG.PM)

The security program lays the groundwork for securing the organization's enterprise and Smart Grid information system assets. Security procedures define how an organization implements the security program.

SG.PM-1 Security Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented security program security policy that addresses—
      i. The objectives, roles, and responsibilities for the security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the security program security policy and associated security program protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the security program security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The information system security policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for the information system in particular, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-1	Moderate: SG.PM-1	High: SG.PM-1

SG.PM-2 Security Program Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops and disseminates an organization-wide security program plan that—
   a. Provides an overview of the requirements for the security program and a description of the security program management requirements in place or planned for meeting those program requirements;
   b. Provides sufficient information about the program management requirements to enable an implementation that is compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
   c. Includes roles, responsibilities, management accountability, coordination among organizational entities, and compliance; and
   d. Is approved by a management authority with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, and individuals;
2. Reviews the organization-wide security program plan on an organization-defined frequency; and
3. Revises the plan to address organizational changes and problems identified during plan implementation or security requirement assessments.

Supplemental Guidance

The security program plan documents the organization-wide program management requirements. The security plans for individual information systems and the organization-wide security program plan together, provide complete coverage for all security requirements employed within the organization.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-2	Moderate: SG.PM-2	High: SG.PM-2

SG.PM-3 Senior Management Authority

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization appoints a senior management authority with the responsibility for the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-3	Moderate: SG.PM-3	High: SG.PM-3

SG.PM-4 Security Architecture

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops a security architecture with consideration for the resulting risk to organizational operations, organizational assets, individuals, and other organizations.

Supplemental Guidance

The integration of security requirements into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the information system development life cycle.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-4	Moderate: SG.PM-4	High: SG.PM-4

SG.PM-5 Risk Management Strategy

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems; and
2. Implements that strategy consistently across the organization.

Supplemental Guidance

An organization-wide risk management strategy should include a specification of the risk tolerance of the organization, guidance on acceptable risk assessment methodologies, and a process for consistently evaluating risk across the organization.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-5	Moderate: SG.PM-5	High: SG.PM-5

SG.PM-6 Security Authorization to Operate Process

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Manages (e.g., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; and
2. Fully integrates the security authorization to operate processes into an organization-wide risk management strategy.

Supplemental Guidance

None.

Requirement Enhancements

None.

Impact Level Allocation

Low: SG.PM-6	Moderate: SG.PM-6	High: SG.PM-6

SG.PM-7 Mission/Business Process Definition

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization defines mission/business processes that include consideration for security and the resulting risk to organizational operations, organizational assets, and individuals.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-7	Moderate: SG.PM-7	High: SG.PM-7

SG.PM-8 Management Accountability

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization defines a framework of management accountability that establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-8	Moderate: SG.PM-8	High: SG.PM-8

3.21 PERSONNEL SECURITY (SG.PS)

Personnel security addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination. The organization screens applicants for critical positions in the operation and maintenance of the Smart Grid information system. The organization may consider implementing a confidentiality or nondisclosure agreement that employees and third-party users of facilities must sign before being granted access to the Smart Grid information system. The organization also documents and implements a process to secure resources and revoke access privileges when personnel terminate.

SG.PS-1 Personnel Security Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented personnel security policy that addresses—
      i. The objectives, roles, and responsibilities for the personnel security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the personnel security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the personnel security policy and associated personnel protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and

3. The organization ensures that the personnel security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The personnel security policy may be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular Smart Grid information system, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-1	Moderate: SG.PS-1	High: SG.PS-1

SG.PS-2 Position Categorization

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations. The organization determines the frequency of the review based on the organization's requirements or regulatory commitments.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-2	Moderate: SG.PS-2	High: SG.PS-2

SG.PS-3 Personnel Screening

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization screens individuals requiring access to the Smart Grid information system before access is authorized. The organization maintains consistency between the screening process and organization-defined policy, regulations, guidance, and the criteria established for the risk designation of the assigned position.

Supplemental Guidance

Basic screening requirements should include:

1. Employment history;
2. Verification of the highest education degree received;
3. Residency;
4. References; and
5. Law enforcement records.

Requirement Enhancements

None.

Additional Considerations

A1. The organization rescreens individuals with access to Smart Grid information systems based on a defined list of conditions requiring rescreening and the frequency of such rescreening.

Impact Level Allocation

Low: SG.PS-3	Moderate: SG.PS-3	High: SG.PS-3

SG.PS-4 Personnel Termination

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. When an employee is terminated, the organization revokes logical and physical access to facilities and systems and ensures that all organization-owned property is returned. Organization-owned documents relating to the Smart Grid information system that are in the employee's possession are transferred to the new authorized owner;
2. All logical and physical access must be terminated at an organization-defined time frame for personnel terminated for cause; and
3. Exit interviews ensure that individuals understand any security constraints imposed by being a former employee and that proper accountability is achieved for all Smart Grid information system-related property.

Supplemental Guidance

Organization-owned property includes Smart Grid information system administration manuals, keys, identification cards, building passes, computers, cell phones, and personal data assistants. Organization-owned documents include field device configuration and operational information and Smart Grid information system network documentation.

Requirement Enhancements

None.

Additional Considerations

A1. The organization implements automated processes to revoke access permissions that are initiated by the termination.

Impact Level Allocation

Low: SG.PS-4	Moderate: SG.PS-4	High: SG.PS-4

SG.PS-5 Personnel Transfer

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization reviews logical and physical access permissions to Smart Grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions; and
2. Complete execution of this requirement occurs within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources.

Supplemental Guidance

Appropriate actions may include:

1. Returning old and issuing new keys, identification cards, and building passes;
2. Closing old accounts and establishing new accounts;
3. Changing Smart Grid information system access authorizations; and
4. Providing access to official records created or managed by the employee at the former work location and in the former accounts.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-5	Moderate: SG.PS-5	High: SG.PS-5

SG.PS-6 Access Agreements

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization completes appropriate agreements for Smart Grid information system access before access is granted. This requirement applies to all parties, including third parties and contractors, who require access to the Smart Grid information system;
2. The organization reviews and updates access agreements periodically; and

3. Signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with the Smart Grid information system to which access is authorized.

Supplemental Guidance

Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-6	Moderate: SG.PS-6	High: SG.PS-6

SG.PS-7 Contractor and Third-Party Personnel Security

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization enforces security requirements for contractor and third-party personnel and monitors service provider behavior and compliance.

Supplemental Guidance

Contactors and third-party providers include service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-7	Moderate: SG.PS-7	High: SG.PS-7

SG.PS-8 Personnel Accountability

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization employs a formal accountability process for personnel failing to comply with established security policies and procedures and identifies disciplinary actions for failing to comply; and

2. The organization ensures that the accountability process complies with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The accountability process can be included as part of the organization's general personnel policies and procedures.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-8	Moderate: SG.PS-8	High: SG.PS-8

SG.PS-9 Personnel Roles

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides employees, contractors, and third parties with expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. Employees and contractors acknowledge understanding by signature.

Impact Level Allocation

Low: SG.PS-9	Moderate: SG.PS-9	High: SG.PS-9

3.22 RISK MANAGEMENT AND ASSESSMENT (SG.RA)

Risk management planning is a key aspect of ensuring that the processes and technical means of securing Smart Grid information systems have fully addressed the risks and vulnerabilities in the Smart Grid information system.

An organization identifies and classifies risks to develop appropriate security measures. Risk identification and classification involves security assessments of Smart Grid information systems and interconnections to identify critical components and any areas weak in security. The risk identification and classification process is continually performed to monitor the Smart Grid information system's compliance status.

SG.RA-1 Risk Assessment Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented risk assessment security policy that addresses—
      i. The objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the risk assessment policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The risk assessment policy also takes into account the organization's risk tolerance level. The risk assessment policy can be included as part of the general security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular Smart Grid information system, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-1	Moderate: SG.RA-1	High: SG.RA-1

SG.RA-2 Risk Management Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops a risk management plan;
2. A management authority reviews and approves the risk management plan; and
3. Risk-reduction mitigation measures are planned and implemented and the results monitored to ensure effectiveness of the organization's risk management plan.

Supplemental Guidance

Risk mitigation measures need to be implemented and the results monitored against planned metrics to ensure the effectiveness of the risk management plan.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-2	Moderate: SG.RA-2	High: SG.RA-2

SG.RA-3 Security Impact Level

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Specifies the information and the information system impact levels;
2. Documents the impact level results (including supporting rationale) in the security plan for the information system; and
3. Reviews the Smart Grid information system and information impact levels on an organization-defined frequency.

Supplemental Guidance

Impact level designation is based on the need, priority, and level of protection required commensurate with sensitivity and impact of the loss of availability, integrity, or confidentiality. Impact level designation may also be based on regulatory requirements, for example, the NERC CIPs. The organization considers safety issues in determining the impact level for the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-3	Moderate: SG.RA-3	High: SG.RA-3

SG.RA-4 Risk Assessment

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Conducts assessments of risk from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and Smart Grid information systems; and
2. Updates risk assessments on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system or environment of operation, or other conditions that may impact the security of the Smart Grid information system.

Supplemental Guidance

Risk assessments take into account vulnerabilities, threat sources, risk tolerance levels, and security mechanisms planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-4	Moderate: SG.RA-4	High: SG.RA-4

SG.RA-5 Risk Assessment Update

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization updates the risk assessment plan on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system, the facilities where the Smart Grid information system resides, or other conditions that may affect the security or authorization-to-operate status of the Smart Grid information system.

Supplemental Guidance

The organization develops and documents specific criteria for what are considered significant changes to the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-5	Moderate: SG.RA-5	High: SG.RA-5

SG.RA-6 Vulnerability Assessment and Awareness

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Monitors and evaluates the Smart Grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a Smart Grid information system;
2. Analyzes vulnerability scan reports and remediates vulnerabilities within an organization-defined time frame based on an assessment of risk;
3. Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other Smart Grid information systems;
4. Updates the Smart Grid information system to address any identified vulnerabilities in accordance with organization's Smart Grid information system maintenance policy; and
5. Updates the list of Smart Grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported.

Supplemental Guidance

Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools to scan for Web-based vulnerabilities, source code reviews, and static analysis of source code). Vulnerability scanning includes scanning for ports, protocols, and services that should not be accessible to users and for improperly configured or incorrectly operating information flow mechanisms.

Requirement Enhancements

1. The organization employs vulnerability scanning tools that include the capability to update the list of Smart Grid information system vulnerabilities scanned; and
2. The organization includes privileged access authorization to organization-defined Smart Grid information system components for selected vulnerability scanning activities to facilitate more thorough scanning.

Additional Considerations

A1. The organization employs automated mechanisms on an organization-defined frequency to detect the presence of unauthorized software on organizational Smart Grid information systems and notifies designated organizational officials;

A2. The organization performs security testing to determine the level of difficulty in circumventing the security requirements of the Smart Grid information system; and

A3. The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in Smart Grid information system vulnerabilities.

Impact Level Allocation

Low: SG.RA-6	Moderate: SG.RA-6 (1)	High: SG.RA-6 (1), (2)

3.23 SMART GRID INFORMATION SYSTEM AND SERVICES ACQUISITION (SG.SA)

Smart Grid information systems and services acquisition covers the contracting and acquiring of system components, software, firmware, and services from employees, contactors, and third parties. A policy with detailed procedures for reviewing acquisitions should reduce the introduction of additional or unknown vulnerabilities into the Smart Grid information system.

SG.SA-1 Smart Grid Information System and Services Acquisition Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented Smart Grid information system and services acquisition security policy that addresses—
      i. The objectives, roles, and responsibilities for the Smart Grid information system and services acquisition security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the Smart Grid information system and services acquisition security program as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the Smart Grid information system and services acquisition policy and associated physical and environmental protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the Smart Grid information system and services acquisition policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The Smart Grid information system and services acquisition policy can be included as part of the general information security policy for the organization. Smart Grid information system and services acquisition procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-1	Moderate: SG.SA-1	High: SG.SA-1

SG.SA-2 Security Policies for Contractors and Third Parties

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. External suppliers and contractors that have an impact on the security of Smart Grid information systems must meet the organization's policy and procedures; and
2. The organization establishes procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the contract.

Supplemental Guidance

The organization considers the increased security risk associated with outsourcing as part of the decision-making process to determine what to outsource and what outsourcing partner to select. Contracts with external suppliers govern physical as well as logical access. The organization considers confidentiality or nondisclosure agreements and intellectual property rights.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-2	Moderate: SG.SA-2	High: SG.SA-2

SG.SA-3 Life-Cycle Support

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization manages the Smart Grid information system using a system development lifecycle methodology that includes security.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-3	Moderate: SG.SA-3	High: SG.SA-3

SG.SA-4 Acquisitions

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization includes security requirements in Smart Grid information system acquisition contracts in accordance with applicable laws, regulations, and organization-defined security policies.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-4	Moderate: SG.SA-4	High: SG.SA-4

SG.SA-5 Smart Grid Information System Documentation

Category: Common Governance, Risk, and Compliance (GRC) Requirement

Requirement

1. Smart Grid information system documentation includes how to configure, install, and use the information system and the information system's security features; and
2. The organization obtains from the contractor/third-party, information describing the functional properties of the security controls employed within the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-5	Moderate: SG.SA-5	High: SG.SA-5

SG.SA-6 Software License Usage Restrictions

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Uses software and associated documentation in accordance with contract agreements and copyright laws; and

2. Controls the use of software and associated documentation protected by quantity licenses and copyrighted material.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-6	Moderate: SG.SA-6	High: SG.SA-6

SG.SA-7 User-Installed Software

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes policies and procedures to manage user installation of software.

Supplemental Guidance

If provided the necessary privileges, users have the ability to install software. The organization's security program identifies the types of software permitted to be downloaded and installed (e.g., updates and security patches to existing software) and types of software prohibited (e.g., software that is free only for personal, not corporate use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-7	Moderate: SG.SA-7	High: SG.SA-7

SG.SA-8 Security Engineering Principles

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization applies security engineering principles in the specification, design, development, and implementation of any Smart Grid information system.

Security engineering principles include:

1. Ongoing secure development education requirements for all developers involved in the Smart Grid information system;

2. Specification of a minimum standard for security;
3. Specification of a minimum standard for privacy;
4. Creation of a threat model for a Smart Grid information system;
5. Updating of product specifications to include mitigations for threats discovered during threat modeling;
6. Use of secure coding practices to reduce common security errors;
7. Testing to validate the effectiveness of secure coding practices;
8. Performance of a final security audit prior to authorization to operate to confirm adherence to security requirements;
9. Creation of a documented and tested security response plan in the event vulnerability is discovered;
10. Creation of a documented and tested privacy response plan in the event vulnerability is discovered; and
11. Performance of a root cause analysis to understand the cause of identified vulnerabilities.

Supplemental Guidance

The application of security engineering principles is primarily targeted at new development Smart Grid information systems or Smart Grid information systems undergoing major upgrades. These principles are integrated into the Smart Grid information system development life cycle. For legacy Smart Grid information systems, the organization applies security engineering principles to Smart Grid information system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the Smart Grid information system. The organization minimizes risk to legacy systems through attack surface reduction and other mitigating controls.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-8	Moderate: SG.SA-8	High: SG.SA-8

SG.SA-9 Developer Configuration Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization requires that Smart Grid information system developers/integrators document and implement a configuration management process that—

1. Manages and controls changes to the Smart Grid information system during design, development, implementation, and operation;

2. Tracks security flaws; and
3. Includes organizational approval of changes.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization requires that Smart Grid information system developers/integrators provide an integrity check of delivered software and firmware.

Impact Level Allocation

Low: SG.SA-9	Moderate: SG.SA-9	High: SG.SA-9

SG.SA-10 Developer Security Testing

Category: Common Technical Requirements, Integrity

Requirement

1. The Smart Grid information system developer creates a security test and evaluation plan;
2. The developer submits the plan to the organization for approval and implements the plan once written approval is obtained;
3. The developer documents the results of the testing and evaluation and submits them to the organization for approval; and
4. The organization does not perform developmental security tests on the production Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization requires that Smart Grid information system developers employ code analysis tools to examine software for common flaws and document the results of the analysis; and

A2. The organization requires that Smart Grid information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.

Impact Level Allocation

Low: SG.SA-10	Moderate: SG.SA-10	High: SG.SA-10

SG.SA-11 Supply Chain Protection

Category: Common Technical Requirements, Integrity

Requirement

The organization protects against supply chain vulnerabilities employing requirements defined to protect the products and services from threats initiated against organizations, people, information, and resources, possibly international in scope, that provides products or services to the organization.

Supplemental Guidance

Supply chain protection helps to protect Smart Grid information systems (including the technology products that compose those Smart Grid information systems) throughout the system development life cycle (e.g., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement).

Requirement Enhancements

None.

Additional Considerations

A1. The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire Smart Grid information system hardware, software, firmware, or services;

A2. The organization uses a diverse set of suppliers for Smart Grid information systems, Smart Grid information system components, technology products, and Smart Grid information system services; and

A3. The organization employs independent analysis and penetration testing against delivered Smart Grid information systems, Smart Grid information system components, and technology products.

Impact Level Allocation

Low: SG.SA-11	Moderate: SG.SA-11	High: SG.SA-11

3.24 SMART GRID INFORMATION SYSTEM AND COMMUNICATION PROTECTION (SG.SC)

Smart Grid information system and communication protection consists of steps taken to protect the Smart Grid information system and the communication links between Smart Grid information system components from cyber intrusions. Although Smart Grid information system and communication protection might include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in SG.PE, Physical and Environmental Security.

SG.SC-1 Smart Grid Information System and Communication Protection Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented Smart Grid information system and communication protection security policy that addresses—
      i. The objectives, roles, and responsibilities for the Smart Grid information system and communication protection security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the Smart Grid information system and communication protection policy as it applies to all of the organizational staff, contractors, and third parties; and
   b. Procedures to address the implementation of the Smart Grid information system and communication protection security policy and associated Smart Grid information system and communication protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the Smart Grid information system and communication protection policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The Smart Grid information system and communication protection policy may be included as part of the general information security policy for the organization. Smart Grid information system and communication protection procedures can be developed for the security program in general and a Smart Grid information system in particular, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-1	Moderate: SG.SC-1	High: SG.SC-1

SG.SC-2 Communications Partitioning

Category: Unique Technical Requirements

Requirement

The Smart Grid information system partitions the communications for telemetry/data acquisition services and management functionality.

Supplemental Guidance

The Smart Grid information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-3 Security Function Isolation

Category: Unique Technical Requirements

Requirement

The Smart Grid information system isolates security functions from nonsecurity functions.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system employs underlying hardware separation mechanisms to facilitate security function isolation; and

A2. The Smart Grid information system isolates security functions (e.g., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.

Impact Level Allocation

Low: SG.SC-3	Moderate: SG.SC-3	High: SG.SC-3

SG.SC-4 Information Remnants

Category: Unique Technical Requirements

Requirement

The Smart Grid information system prevents unauthorized or unintended information transfer via shared Smart Grid information system resources.

Supplemental Guidance

Control of Smart Grid information system remnants, sometimes referred to as object reuse, or data remnants, prevents information from being available to any current user/role/process that obtains access to a shared Smart Grid information system resource after that resource has been released back to the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-4	High: SG.SC-4

SG.SC-5 Denial-of-Service Protection

Category: Unique Technical Requirements

Requirement

The Smart Grid information system mitigates or limits the effects of denial-of-service attacks based on an organization-defined list of denial-of-service attacks.

Supplemental Guidance

Network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial-of-service attacks.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system restricts the ability of users to launch denial-of-service attacks against other Smart Grid information systems or networks; and

A2. The Smart Grid information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

Impact Level Allocation

Low: SG.SC-5	Moderate: SG.SC-5	High: SG.SC-5

SG.SC-6 Resource Priority

Category: Unique Technical Requirements

Requirement

The Smart Grid information system prioritizes the use of resources.

Supplemental Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the Smart Grid information system servicing any higher-priority process. This requirement does not apply to components in the Smart Grid information system for which only a single user/role exists.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-7 Boundary Protection

Category: Unique Technical Requirements

Requirement

1. The organization defines the boundary of the Smart Grid information system;
2. The Smart Grid information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
3. The Smart Grid information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices;
4. The managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information; and
5. The organization prevents public access into the organization's internal Smart Grid information system networks except as appropriately mediated.

Supplemental Guidance

Managed interfaces employing boundary protection devices include proxies, gateways, routers, firewalls, guards, or encrypted tunnels.

Requirement Enhancements

1. The Smart Grid information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception);
2. The Smart Grid information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination; and
3. Communications to/from Smart Grid information system components shall be restricted to specific components in the Smart Grid information system. Communications shall not be permitted to/from any non-Smart Grid system unless separated by a controlled logical/physical interface.

Additional Considerations

A1. The organization prevents the unauthorized release of information outside the Smart Grid information system boundary or any unauthorized communication through the Smart Grid information system boundary when an operational failure occurs of the boundary protection mechanisms;

A2. The organization prevents the unauthorized exfiltration of information across managed interfaces;

A3. The Smart Grid information system routes internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices;

A4. The organization limits the number of access points to the Smart Grid information system to allow for better monitoring of inbound and outbound network traffic;

A5. Smart Grid information system boundary protections at any designated alternate processing/control sites provide the same levels of protection as that of the primary site; and

A6. The Smart Grid information system fails securely in the event of an operational failure of a boundary protection device.

Impact Level Allocation

Low: SG.SC-7	Moderate: SG.SC-7 (1), (2), (3)	High: SG.SC-7 (1), (2), (3)

SG.SC-8 Communication Integrity

Category: Unique Technical Requirements

Requirement

The Smart Grid information system protects the integrity of electronically communicated information.

Supplemental Guidance

None.

Requirement Enhancements

1. The organization employs cryptographic mechanisms to ensure integrity.

Additional Considerations

A1. The Smart Grid information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-8 (1)	High: SG.SC-8 (1)

SG.SC-9 Communication Confidentiality

Category: Unique Technical Requirements

Requirement

The Smart Grid information system protects the confidentiality of communicated information.

Supplemental Guidance

None.

Requirement Enhancements

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-9 (1)	High: SG.SC-9 (1)

SG.SC-10 Trusted Path

Category: Unique Technical Requirements

Requirement

The Smart Grid information system establishes a trusted communications path between the user and the Smart Grid information system.

Supplemental Guidance

A trusted path is the means by which a user and target of evaluation security functionality can communicate with the necessary confidence.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-11 Cryptographic Key Establishment and Management

Category: Common Technical Requirements, Confidentiality

Requirement

The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance

Key establishment includes a key generation process in accordance with a specified algorithm and key sizes, and key sizes based on an assigned standard. Key generation must be performed using an appropriate random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution.

Requirement Enhancements

1. The organization maintains availability of information in the event of the loss of cryptographic keys by users. *See* Chapter 4 for key management requirements.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-11	Moderate: SG.SC-11 (1)	High: SG.SC-11 (1)

SG.SC-12 Use of Validated Cryptography

Category: Common Technical Requirements, Confidentiality

Requirement

All of the cryptography and other security functions (e.g., hashes, random number generators, etc.) that are required for use in a Smart Grid information system shall be NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes.

Supplemental Guidance

For a list of current FIPS-approved or allowed cryptography, *see* Chapter Four Cryptography and Key Management.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-12	Moderate: SG.SC-12	High: SG.SC-12

SG.SC-13 Collaborative Computing

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops, disseminates, and periodically reviews and updates on an organization-defined frequency a collaborative computing policy.

Supplemental Guidance

Collaborative computing mechanisms include video and audio conferencing capabilities or instant messaging technologies. Explicit indication of use includes signals to local users when cameras and/or microphones are activated.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-13	Moderate: SG.SC-13	High: SG.SC-13

SG.SC-14 Transmission of Security Parameters

Category: Unique Technical Requirements

Requirement

The Smart Grid information system reliably associates security parameters with information exchanged between the enterprise information systems and the Smart Grid information system.

Supplemental Guidance

Security parameters may be explicitly or implicitly associated with the information contained within the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system validates the integrity of security parameters exchanged between Smart Grid information systems.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-15 Public Key Infrastructure Certificates

Category: Common Technical Requirements, Confidentiality

Requirement

For Smart Grid information systems that implement a public key infrastructure, the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-15	Moderate: SG.SC-15	High: SG.SC-15

SG.SC-16 Mobile Code

Category: Common Technical Requirements, Confidentiality

Requirement

The organization—

1. Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the Smart Grid information system if used maliciously;
2. Documents, monitors, and manages the use of mobile code within the Smart Grid information system; and
3. A management authority authorizes the use of mobile code.

Supplemental Guidance

Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance need to apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-16	High: SG.SC-16

SG.SC-17 Voice-Over Internet Protocol

Category: Unique Technical Requirements

Requirement

The organization—

1. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-17	High: SG.SC-17

SG.SC-18 System Connections

Category: Common Technical Requirements, Confidentiality

Requirement

All external Smart Grid information system and communication connections are identified and protected from tampering or damage.

Supplemental Guidance

External access point connections to the Smart Grid information system need to be secured to protect the Smart Grid information system. Access points include any externally connected communication end point (for example, dial-up modems).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-18	Moderate: SG.SC-18	High: SG.SC-18

SG.SC-19 Security Roles

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system design and implementation specifies the security roles and responsibilities for the users of the Smart Grid information system.

Supplemental Guidance

Security roles and responsibilities for Smart Grid information system users need to be specified, defined, and implemented based on the sensitivity of the information handled by the user. These roles may be defined for specific job descriptions or for individuals.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-19	Moderate: SG.SC-19	High: SG.SC-19

SG.SC-20 Message Authenticity

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system provides mechanisms to protect the authenticity of device-to-device communications.

Supplemental Guidance

Message authentication provides protection from malformed traffic, misconfigured devices, and malicious entities.

Requirement Enhancements

None.

Additional Considerations

A1. Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.

Impact Level Allocation

Low: SG.SC-20	Moderate: SG.SC-20	High: SG.SC-20

SG.SC-21 Secure Name/Address Resolution Service

Category: Common Technical Requirements, Integrity

Requirement

The organization is responsible for—

1. Configuring systems that provide name/address resolution to supply additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries; and
2. Configuring systems that provide name/address resolution to Smart Grid information systems, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-21	Moderate: SG.SC-21	High: SG.SC-21

SG.SC-22 Fail in Known State

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system fails to a known state for defined failures.

Supplemental Guidance

Failure in a known state can be interpreted by organizations in the context of safety or security in accordance with the organization's mission/business/operational needs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the Smart Grid information system or a component of the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system preserves defined system state information in failure.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-22	High: SG.SC-22

SG.SC-23 Thin Nodes

Category: Unique Technical Requirements

Requirement

The Smart Grid information system employs processing components that have minimal functionality and data storage.

Supplemental Guidance

The deployment of Smart Grid information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the number of endpoints to be secured and may reduce the exposure of information, Smart Grid information systems, and services to a successful attack.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-24 Honeypots

Category: Unique Technical Requirements

Requirement

The Smart Grid information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system includes components that proactively seek to identify Web-based malicious code.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-25 Operating System-Independent Applications

Category: Unique Technical Requirements

Requirement

The Smart Grid information system includes organization-defined applications that are independent of the operating system.

Supplemental Guidance

Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, thus increasing the availability for critical functionality while an organization is under an attack exploiting vulnerabilities in a given operating system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-26 Confidentiality of Information at Rest

Category: Unique Technical Requirements

Requirement

The Smart Grid information system employs cryptographic mechanisms for all critical security parameters (e.g., cryptographic keys, passwords, security configurations) to prevent unauthorized disclosure of information at rest.

Supplemental Guidance

For a list of current FIPS-approved or allowed cryptography, *see* Chapter Four Cryptography and Key Management.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-26	High: SG.SC-26

SG.SC-27 Heterogeneity

Category: Unique Technical Requirements

Requirement

The organization employs diverse technologies in the implementation of the Smart Grid information system.

Supplemental Guidance

Increasing the diversity of technologies within the Smart Grid information system reduces the impact from the exploitation of a specific technology.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-28 Virtualization Techniques

Category: Unique Technical Requirements

Requirement

The organization employs virtualization techniques to present gateway components into Smart Grid information system environments as other types of components, or components with differing configurations.

Supplemental Guidance

Virtualization techniques provide organizations with the ability to disguise gateway components into Smart Grid information system environments, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications;

A2. The organization changes the diversity of operating systems and applications on an organization-defined frequency; and

A3. The organization employs randomness in the implementation of the virtualization.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected

SG.SC-29 Application Partitioning

Category: Unique Technical Requirements

Requirement

The Smart Grid information system separates user functionality (including user interface services) from Smart Grid information system management functionality.

Supplemental Guidance

Smart Grid information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from Smart Grid information system management functionality is either physical or logical.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system prevents the presentation of Smart Grid information system management-related functionality at an interface for general (i.e., non-privileged) users.

Additional Considerations Supplemental Guidance

The intent of this additional consideration is to ensure that administration options are not available to general users. For example, administration options are not presented until the user has appropriately established a session with administrator privileges.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: SG.SC-29

SG.SC-30 Smart Grid Information System Partitioning

Category: Common Technical Requirements, Integrity

Requirement

The organization partitions the Smart Grid information system into components residing in separate physical or logical domains (or environments).

Supplemental Guidance

An organizational assessment of risk guides the partitioning of Smart Grid information system components into separate domains (or environments).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-30	High: SG.SC-30

3.25 SMART GRID INFORMATION SYSTEM AND INFORMATION INTEGRITY (SG.SI)

Maintaining a Smart Grid information system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security requirements described under the Smart Grid information system and information integrity family provide policy and procedure for identifying, reporting, and correcting Smart Grid information system flaws. Requirements exist for malicious code detection. Also provided are requirements for receiving security alerts and advisories and the verification of security functions on the Smart Grid information system. In addition, requirements within this family detect and protect against unauthorized changes to software and data; restrict data input and output; check the accuracy, completeness, and validity of data; and handle error conditions.

SG.SI-1 Smart Grid Information System and Information Integrity Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
    a. A documented Smart Grid information system and information integrity security policy that addresses—
        i. The objectives, roles, and responsibilities for the Smart Grid information system and information integrity security program as it relates to protecting the organization's personnel and assets; and
        ii. The scope of the Smart Grid information system and information integrity security program as it applies to all of the organizational staff, contractors, and third parties; and

b. Procedures to address the implementation of the Smart Grid information system and information integrity security policy and associated Smart Grid information system and information integrity protection requirements;

2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the Smart Grid information system and information integrity policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The Smart Grid information system and information integrity policy can be included as part of the general control security policy for the organization. Smart Grid information system and information integrity procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SI-1	Moderate: SG.SI-1	High: SG.SI-1

SG.SI-2 Flaw Remediation

Category: Common Technical Requirements, Integrity

Requirement

The organization—

1. Identifies, reports, and corrects Smart Grid information system flaws;
2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational Smart Grid information systems before installation; and
3. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance

The organization identifies Smart Grid information systems containing software and firmware (including operating system software) affected by recently announced flaws (and potential vulnerabilities resulting from those flaws). Flaws discovered during security assessments, continuous monitoring, or under incident response activities also need to be addressed.

Requirement Enhancements

None.

Additional Considerations

A1. The organization centrally manages the flaw remediation process. Organizations consider the risk of employing automated flaw remediation processes on a Smart Grid information system;

A2. The organization employs automated mechanisms on an organization-defined frequency and on demand to determine the state of Smart Grid information system components with regard to flaw remediation; and

A3. The organization employs automated patch management tools to facilitate flaw remediation to organization-defined Smart Grid information system components.

Impact Level Allocation

Low: SG.SI-2	Moderate: SG.SI-2	High: SG.SI-2

SG.SI-3 Malicious Code and Spam Protection

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization—
   a. Implements malicious code protection mechanisms; and
   b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; and
2. The Smart Grid information system prevents users from circumventing malicious code protection capabilities.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization centrally manages malicious code protection mechanisms;

A2. The Smart Grid information system updates malicious code protection mechanisms in accordance with organization-defined policies and procedures;

A3. The organization configures malicious code protection methods to perform periodic scans of the Smart Grid information system on an organization-defined frequency;

A4. The use of mechanisms to centrally manage malicious code protection must not degrade the operational performance of the Smart Grid information system; and

A5. The organization employs spam protection mechanisms at system entry points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, or other common means.

Impact Level Allocation

Low: SG.SI-3	Moderate: SG.SI-3	High: SG.SI-3

SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization monitors events on the Smart Grid information system to detect attacks, unauthorized activities or conditions, and non-malicious errors.

Supplemental Guidance

Smart Grid information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, and network forensic analysis tools). The granularity of the information collected can be determined by the organization based on its monitoring objectives and the capability of the Smart Grid information system to support such activities.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system notifies a defined list of incident response personnel;

A2. The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion;

A3. The organization tests/exercises intrusion monitoring tools on a defined time period;

A4. The organization interconnects and configures individual intrusion detection tools into a Smart Grid system-wide intrusion detection system using common protocols;

A5. The Smart Grid information system provides a real-time alert when indications of compromise or potential compromise occur; and

A6. The Smart Grid information system prevents users from circumventing host-based intrusion detection and prevention capabilities.

Impact Level Allocation

Low: SG.SI-4	Moderate: SG.SI-4	High: SG.SI-4

SG.SI-5 Security Alerts and Advisories

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Receives Smart Grid information system security alerts, advisories, and directives from external organizations; and

2. Generates and disseminates internal security alerts, advisories, and directives as deemed necessary.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to disseminate security alert and advisory information throughout the organization.

Impact Level Allocation

Low: SG.SI-5	Moderate: SG.SI-5	High: SG.SI-5

SG.SI-6 Security Functionality Verification

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization verifies the correct operation of security functions within the Smart Grid information system upon—
   a. Smart Grid information system startup and restart; and
   b. Command by user with appropriate privilege at an organization-defined frequency; and
2. The Smart Grid information system notifies the management authority when anomalies are discovered.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to provide notification of failed automated security tests; and

A2. The organization employs automated mechanisms to support management of distributed security testing.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SI-6	High: SG.SI-6

SG.SI-7 Software and Information Integrity

Category: Unique Technical Requirements

Requirement

The Smart Grid information system monitors and detects unauthorized changes to software and information.

Supplemental Guidance

The organization employs integrity verification techniques on the Smart Grid information system to look for evidence of information tampering, errors, and/or omissions.

Requirement Enhancements

1. The organization reassesses the integrity of software and information by performing on an organization-defined frequency integrity scans of the Smart Grid information system.

Additional Considerations

A1. The organization employs centrally managed integrity verification tools; and

A2. The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SI-7 (1)	High: SG.SI-7 (1)

SG.SI-8 Information Input Validation

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system employs mechanisms to check information for accuracy, completeness, validity, and authenticity.

Supplemental Guidance

Rules for checking the valid syntax of Smart Grid information system input (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SI-8	High: SG.SI-8

SG.SI-9 Error Handling

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system—

1. Identifies error conditions; and
2. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries.

Supplemental Guidance

The extent to which the Smart Grid information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SI-9	Moderate: SG.SI-9	High: SG.SI-9

CHAPTER FOUR
CRYPTOGRAPHY AND KEY MANAGEMENT

This chapter identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives. The identified alternatives may be existing standards, methods, or technologies, and their optimal adaptations for the Smart Grid. Where alternatives do not exist, the subgroup has identified gaps where new standards and/or technologies should be developed for the industry.

4.1 SMART GRID CRYPTOGRAPHY AND KEY MANAGEMENT ISSUES

4.1.1 General Constraining Issues

4.1.1.1 Computational Constraints

Some Smart Grid devices, particularly residential meters and in-home devices, may be limited in their computational power and/or ability to store cryptographic materials. The advent of low-cost semiconductors, including low-cost embedded processors with built-in cryptographic capabilities, will, however, ease some such constraints when the supply chain—from manufacturing to deployment to operation—absorbs this technology and aligns it with key management systems for Smart Grid operations. We can expect that most future devices connected to the Smart Grid will have basic cryptographic capabilities, including the ability to support symmetric ciphers for authentication and/or encryption. Public-key cryptography may be supported either in hardware by means of a cryptography co-processor or, as long as it is performed infrequently (i.e., less than once per hour), it can be supported in software. We also note that the use of low-cost hardware with embedded cryptography support is a necessary but not wholly sufficient step toward achieving high availability, integrity, and confidentiality in the Smart Grid. A trustworthy and unencumbered implementation of cryptography that is suitable (both computationally and resource-wise) for deployment in the Smart Grid would benefit all stakeholders in Smart Grid deployments.

4.1.1.2 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 Advanced Encryption Standard (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 it must be performed before encryption—and this must be taken into account in designing the network stack.

Integrity protection as provided by an efficient Cipher-Based Message Authentication Code (CMAC) adds a fixed overhead to every message, typically 64 or 96 bits. On slow channels that communicate primarily short messages, this overhead can be significant. For instance, the SEL Mirrored Bits® protocol for line protection continuously exchanges 8-bit messages. Protecting these messages would markedly impact latency unless the channel bandwidth is 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 or keys that are used for an extended period of time, as with the Internet Key Exchange (IKE) protocol, certificate exchange can be practical over even slow channels. However, if the certificate-based key-establishment exchange is time critical, protocols like IKE that exchange multiple messages before arriving at a pre-shared key may be too costly, even if the size of the certificate is minimal.

4.1.1.3 Connectivity

Standard Public Key Infrastructure (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, Online Certificate Status Protocol (OCSP) servers, etc. Many connections between Smart Grid devices will have much longer durations (often permanent) than typical connections on the Internet.

4.1.2 General Cryptography Issues

4.1.2.1 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.

4.1.2.2 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 include a decision about which block ciphers (e.g., 3DES, AES) are appropriate and in which modes (CBC, CTR, etc.), the key sizes, to be used, and the asymmetric ciphers (e.g., ECC, RSA, etc.) that could form the basis for many authentication operations. The United States Federal Information Processing Standard (FIPS), the NIST Special Publications (SPs), and the NSA Suite B Cryptography strategy provide secure, standard methods for achieving interoperability. Device profile, data temporality/criticality/value should also play a role in cipher and key strength selection. FIPS 140-2 specifies requirements for validating cryptographic implementations for conformance to the FIPS and SPs.

4.1.2.3 Key Management Issues

All security protocols rely on the existence of a security association (SA). From RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*, "SAs contain all the information required for execution of various network security services." An SA can be authenticated or unauthenticated. The establishment of an authenticated SA requires that at least one party possess some sort of credential that can be used to provide assurance of identity or device attributes to others. In general two types of credentials are common: secret keys that are shared between entities (e.g., devices), and (digital) public key certificates for key establishment (i.e., for transporting or computing the secret keys that are to be shared). Public key certificates

are used to bind user or device names to a public key through some third-party attestation model, such as a PKI.

It is not uncommon for vendors to offer solutions using secure protocols by implementing IPSec with AES and calling it a day, leaving customers to figure out how to provision all their devices with secret keys or digital certificates. It is worthwhile to ask the question, "Is it better to provision devices with secret keys or with certificates?" The provisioning of secret keys (i.e., symmetric keys) can be a very expensive process, with security vulnerabilities not present when using digital certificates. The main reason for this is that with symmetric keys, the keys need to be transported from the device where they were generated and then inserted into at least one other device; typically, a different key is required for each pair of communicating devices. Care needs to be taken to ensure that the key provisioning is coordinated so that each device receives the appropriate keys—a process that is prone to human error and subject to insider attacks. There are hardware solutions for secure key transport and loading, but these can require a great deal of operational overhead and are typically cost-prohibitive for all but the smallest systems. All of this overhead and risk can be multiplied several times if each device is to have several independent security associations, each requiring a different key. Of course, techniques like those used by Kerberos can eliminate much of the manual effort and associated cost, but Kerberos cannot provide the high-availability solution when network or power outages prevent either side of the communication link from accessing the key distribution center (KDC).

The provisioning of digital certificates can be a much more cost-effective solution, because this does not require the level of coordination posed by symmetric key provisioning. With digital certificates, each device typically only needs one certificate for key establishment, and one key establishment private key that never leaves the device, once installed. Some products generate, store, and use the private key in a FIPS-140 hardware security module (HSM). In systems like this where the private key never leaves the hardware security module, it is not hard to see how such systems can offer higher levels of security with lower associated operational costs. Of course this explanation is a bit simplistic. For example, certificate provisioning involves several steps, including the generation of a key pair with suitable entropy, the generation of a certificate signing request (CSR) that is forwarded to a Registration Authority (RA) device, appropriate vetting of the CSR by the RA, and forwarding the CSR (signed by the RA) to the Certificate Authority (CA), which issues the certificate and stores it in a repository and/or sends it back to the subject (i.e., the device authorized to use the private key). CAs need to be secured, RA operators need to be vetted, certificate revocation methods need to be maintained, certificate policies need to be defined, and so on. Operating a PKI for generating and handling certificates can also require a significant amount of overhead and is typically not appropriate for small and some midsized systems. A PKI-based solution, which can have a high cost of entry, but requires only one certificate per device (as opposed to one key per pair of communicating devices), and may be more appropriate for large systems, depending on the number of possible communicating pairs of devices. In fact, the largest users of digital certificates are the Department of Defense (DoD) and large enterprises.

4.1.2.4 Summarized Issues with PKI

A PKI is not without its issues. Most issues fall into two categories: First, a PKI can be complex to operate; and second, PKI policies are not globally understood. Both categories can be attributed to the fact that Pa KI is extremely flexible. In fact, a PKI is more of a framework than

an actual solution. A PKI allows each organization to set its own policies, to define its own certificate policy Object Identifiers (CP OIDs), to determine how certificate requests are vetted, how private keys are protected, how CA hierarchies are constructed, and the allowable life of certificates and cached certificates' status information. It is exactly because of this flexibility that PKI can be expensive. Organizations that wish to deploy a PKI need to address each of these and issues, and evaluate them against their own operational requirements to determine their own specific "flavor" of PKI. Then when the organization decides to interoperate with other organizations, they need to undergo a typically expensive effort to evaluate the remote organization's PKI, compare it against the local organization's requirements, determine if either side needs to make any changes, and create an appropriate policy mapping to be used in cross-domain certificates.

Another issue affecting a PKI is the need for certificate revocation and determining the validity of a certificate before accepting it from an entity (e.g. network node) that needs to be authenticated. Typically, this is accomplished by the Relying Party (RP), the node that is performing the authentication, checking the certificate revocation list (CRL) or checking with an online certificate status server. Both of these methods typically require connectivity to a backend server. This would appear to have the same availability issues as typical server-based authentication methods, such as Kerberos- or RADIUS-based methods. However, this is not necessarily true. Methods to mitigate the reliance on infrastructure components to validate certificates are discussed under "PKI High Availability Issues [§4.1.2.4.1].

There is also the issue of trust management. A PKI is often criticized for requiring one root CA to be trusted by everyone, but this is not actually the case. It is more common that each organization operates its own root and then cross-signs other roots (or other CAs) when they determine a need for inter-domain operations. For Smart Grid, each utility could operate their own PKI (or outsource it, if they wish). Those utility organizations that need to interoperate can cross-sign their appropriate CAs. Furthermore, it would be possible for the Smart Grid community to establish one or more bridge CAs so that utility organizations would each only have to cross-sign once with the bridge. All cross-signed certificates can and should be constrained to a specific set of applications or use cases. Trust management is not a trivial issue and is discussed in more detail under "Trust Management" [§4.1.2.4.3].

4.1.2.4.1 PKI High-Availability Issues

The seeming drawback to PKI in needing to authenticate certificates through an online server need not be seen as a major issue. Network nodes can obtain certificate status assertions periodically (when they are connected to the network) and use them at a later time when authenticating with another node. In general, with this method, the node would present its certificate status assertion along with its certificate when performing authentication; Transport Layer Security (TLS) already supports this functionality. This is commonly referred to as Online Certificate Status Protocol (OCSP) stapling. In this way, very high availability could be achieved even when the authenticating nodes are completely isolated from the rest of the network.

Symmetric key methods of establishing SAs can be classified into two general categories: server-based credentials, and preconfigured credentials. With server-based systems, such as Kerberos or RADIUS, connectivity to the security server is required for establishing a security association. Of course, these servers can be duplicated a few times to have a high level of assurance that at least one of them would always be available, but considering the size of the grid, this is not likely

to offer an affordable solution that can ensure that needed SAs can always be established in the case of various system outages. Duplication of the security server also introduces unnecessary vulnerabilities. As it is impossible to ensure that every node will always have access to a security server, this type of solution may not always be suitable for high-availability use cases.

The preconfigured SA class solution requires that each device be provisioned with the credential (usually a secret key or a hash of the secret key) of every entity with whom that the device will need to authenticate. This solution, for all but the smallest systems, is likely to be excessively costly, subject to human error, and encumbered with significant vulnerabilities, due to the replication of so many credentials.

Digital certificates, on the other hand, have the distinct advantage that the first node can establish an Authenticated SA with any other node that has a trust relationship with the first node's issuing CA. This trust relationship may be direct (i.e., it is stored as a trust anchor on the second node), or it may result from a certificate chain.

In the case where a chain of certificates is needed to establish trust, it is typical for devices to carry a few types of certificates. The device would need a chain of certificates beginning with its trust anchor (TA) and ending with its own certificate. The device may also carry one or more certificate chains beginning with the TA and ending with a remote domain's TA or CA. The device can store its own recent certificate status. In a system where every node carries such data, it is possible for all "trustable" nodes to perform mutual authentication, even in the complete absence of any network infrastructure.

With using a PKI, it is important for a Relying Party (RP) to verify the status of the certificate being validated. Normally, the RP would check a CRL or verify the certificate status with an OCSP responder. Another method, proposed in RFC 4366, but not widely deployed, involves a technique called OCSP stapling. With OCSP stapling, a certificate subject obtains an OCSP response (i.e., a certificate status assertion) for its own certificate and provides it to the RP. It is typical for OCSP responses to be cached for a predetermined time, as is similarly done with CRLs. Therefore, it is possible for devices to get OCSP responses for their own certificates when in reach of network infrastructure resources and provide them to RPs at a later time. One typical strategy is for devices to attempt to obtain OCSP responses daily and cache them. Another strategy is for devices to obtain an OCSP response whenever a validation is required.

For a complete, high-assurance solution, the digital certificates must carry not only authentication credentials, but also authorization credentials. This can be accomplished in one of several ways. There are several certificate parameters that can be used to encode authorization information. Some options include Subject Distinguished Name, Extended Key Usage (EKU), the WLAN SSID extension, Certificate Policy extension, and other attributes defined in RFC 4334 and other RFCs. A complete analysis of which fields to use and how to use them would be a large undertaking suitable for its own paper on the topic. Briefly, however, it is worth mentioning that the distinguished names (DNs) option offers many subfields which could be used to indicate a type of device or a type of application that this certificate subject is authorized to communicate with. The EKU field provides an indication of protocols for which the certificate is authorized (e.g., IPSec, TLS, and Secure Shell or SSH). The WLAN SSID extension can be used to limit a device to only access listed SSIDs. The most promising extension for authorization is probably the Certificate Policy (CP) extension. The CP extension indicates to the RP the applicability of a certificate to a particular purpose.

It is also possible to encode authorization credentials into either the subject's identity certificate (which binds the subject's identity to the public key) or to encode the authorization credential into a separate attribute certificate. Typically, organizations need to weigh the benefits of needing to support only one set of certificates with the issues surrounding reissuing identity certificates every time a subject's authorization credential changes. When issuing credentials to people, this is a valid issue. For devices it is rare that authorization credentials will need to change; thus, placing the authorization credentials in the identity certificates poses few disadvantages.

With proper chains of certificates, recent OCSP responses, and authorization credentials, it is possible to provide very high assurance systems that allow two entities to authenticate for authorized services, even when significant portions of the network infrastructure are unavailable.

4.1.2.4.2 Hardware Security Module and PKI

As mentioned above, it is possible to generate and store the secret or private keys used in public key-based cryptography in an HSM. It is reasonable to ask if such devices will drive up costs for price-sensitive Smart Grid components such as sensors. Currently, the smartcard market is driving down the price of chips that can securely store keys, as well as perform public key operations. Such chips can cost only a couple of dollars when purchased in large quantities. Not only does this provide security benefits, but in addition, such chips can offload processing from the embedded device CPU during cryptographic operations. CPU processing capabilities should not then be a significant obstacle to the use of public key cryptography for new (non-legacy) devices. It is typical for public key cryptography to be required only during SA establishment. After the SA has been established, symmetric key cryptography is more favorable. However it is recognized that the supply chain (from manufacture to deployment) and asset owner operations require more Smart Grid-focused key management and encryption standards before the broad use of such technology across the entire infrastructure.

4.1.2.4.3 Trust Management

A number of high-level trust management models can be considered: strict hierarchy, full mesh, or federated trust management[22], for example. When multiple organizations are endeavoring to provide a rich web of connectivity that extends across the resources of the multiple agencies, the strict hierarchy model can quickly be eliminated, because it is typically very difficult to get everyone involved to agree on who they can all trust, and under what policies this "trusted" party should operate. Just as importantly, a strict hierarchy relies on the absolute security of the central "root of trust," because a breach of the central root destroys the security of the whole system. This leaves the mesh model and the federated trust management model. The mesh model is likely to be too expensive. In fact, the federated model brings together the best features of a hierarchy and a mesh. A PKI federation is an abstract term that is usually taken to mean a domain that controls (whether owned or outsourced) its own PKI components and policies and that decides for itself its internal structure—usually, but not always a hierarchy. The domain decides when and how to cross-sign with other domains, whether directly or through a regional bridge. Such a federated approach is really the only reasonable solution for large inter-domain systems.

[22] See Housley, Polk; "Planning for PKI" 2001 Chapter 10, "Building and Validating Certification Paths"

In general any two domains should be allowed to cross-sign as they see fit. However, the activity of cross-signing with many other domains can result in significant overhead. Utilitiy companies may wish to form regional consortiums that would provide bridging services for its member utility companies to help alleviate this concern.

Small utilities could outsource their PKI. This is not necessarily the same as going to a public PKI provider, such as a large CA organization, and getting an "Internet model" certificate. With the Internet model, a certificate mainly proves that you are the rightful owner of the domain name listed in your certificate. For Smart Grid, this is probably not sufficient. Certificates should be used to prove ownership, as well as being used for authorization credentials. Smart Grid certificates could be issued under Smart Grid–sanctioned policies and could carry authorization credentials.

IEEE 802.16 (WiMAX) PKI certificates, by comparison, do not prove ownership; they can only be used to prove that the entity with the corresponding private key is the entity listed in the certificate. An AAA server must then be queried to obtain the authorization credential of the device.

4.1.2.4.4 Need for a Model Policy

A certificate policy is a document that describes the policies under which a particular certificate was issued. A typical CP document contains a rich set of requirements for all PKI participants, including those that are ascribed to the Relying Party. A CP document also contains legal statements, such as liability limits that the PKI is willing to accept. RFC 3647 provides an outline and description for a template CP document. Most PKIs follow this template.

A certificate reflects the CP that it was issued under by including a Certificate Policy Extension. The CP Extension contains an Object ID that is a globally unique number string (also referred to as an arc) that can be used by an RP to trace back to a CP document. The RP can then determine information about the certificate, such as the level of assurance with which it was issued, how it was vetted, how the private keys of the CA are protected, and whether the RP should obtain recent status information about the certificate.

A CP OID also indicates the applicability of a certificate to a particular application. A PKI can use different CP OIDs for different device types to clearly distinguish between those device types, which reduces the need to rely on strict naming conventions. The RP can be configured with acceptable CP OIDs, eliminating the need for the RP to actually obtain and read the CP document.

4.1.2.4.5 Certificate Lifetimes

It is tempting to issue certificates with lifetimes of 50 years or longer. This seems convenient, because they are out there and no one needs to worry about them for 50 years. However, the use of 50-year certificates would have serious implications in the future. Revoked certificates must remain on a CRL until the certificate expires. This can create very large CRLs that are an issue for those resource-constrained devices found throughout the Smart Grid.

Certificate lifetimes should be set to an amount of time commensurate with system risks and application; however as an upper bound it is recommended a maximum of 10 years not be surpassed. An approaching expiration date should trigger a flag in the system, urging

replacement of the certificate—a scheme that would reduce the burden of storing a large number of revoked certificates in the CRL.

A more appropriate solution would be to determine reasonable lifetimes for all certificates. This is not a trivial issue, and different organizations, for a variety of reasons, will select different lifetimes for similar certificates. The following points address a few considerations for three different types of certificates:

- ***Manufacturers' Device Management Certificates***. These certificates are installed into devices by the manufacturer; they typically bind the make, model, and serial number of a device to a public key and are used to prove the nature of the device to a remote entity. These certificates typically offer no trust in themselves (other than to say what the device is); that is, they do not provide any authorization credentials. They can be used to determine if the device is allowed access to given resources. It is common to use this certificate to find a record in an AAA server that indicates the authorization credentials of the subject device. For such certificates, RFC 5280 (§ 4.1.2.5) recommends using a Generalized Time value of 99991231235959Z for the expiration date (i.e., the notAfter date). This indicates that the certificate has no valid expiration date.
- ***User Certificates***. One of the main reasons to select a certificate lifetime is to manage the size of the associated CRLs. Factors that can affect the total number of revoked certificates in a domain include the total number of certificates issued, the certificate lifetimes, and employee turnover. Regardless of how many certificates are currently revoked, there are several other ways to manage CRL sizes. Some of these methods include partitioning the certificates across multiple CAs, scoping CRLs to portions of the user base, and implementing multiple CRL issuers per CA. The operator's Policy Management authority will have to take these considerations into account and derive their own policy. Two to three years are common lifetimes for user certificates. For example, the DoD certificate policy specifies maximum certificate lifetimes of three years for high and medium assurance certificates.
- ***Operator-Issued Device Certificates***. As mentioned above for operator (e.g., utility) issued device certificates, such limitless lifetimes would not be appropriate, due to issues with maintaining CRLs. Because device turnover is typically less frequent than user turnover, it is reasonable to issue these certificates with longer lifetimes. A reasonable range to consider would be three to six years. Going much beyond six years may introduce key lifetime issues.

This is not a trivial topic, and future work should be done to ensure that appropriate guidelines and best practices are established for the Smart Grid community.

4.1.2.5 Elliptic Curve Cryptography

The National Security Agency (NSA) has initiated a Cryptographic Interoperability Strategy (CIS) for U.S. government systems. Part of this strategy has been to select a set of NIST-approved cryptographic techniques, known as NSA Suite B, and foster the adoption of these techniques through inclusion into standards of widely-used protocols, such as the Internet Engineering Task Force (IETF) TLS, Secure/Multipurpose Internet Mail Extensions (S/MIME), IPSec, and SSH. NSA Suite B consists of the following NIST-approved techniques:

- ***Encryption***. Advanced Encryption Standard – FIPS PUB 197 (with keys sizes of 128 and 256 bits)[23]
- ***Key Exchange***. The Ephemeral Unified Model and the One-Pass Diffie-Hellman key agreement schemes (two of several ECDH schemes) – 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 pertaining to the adoption of ECC. To mitigate these issues NSA has stated [§4.4-25]:

> 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.[24]

A number of questions arise when considering this license for Smart Grid use:

1. How can vendors wishing to develop Suite B–enabled commercial off-the-shelf (COTS) products for use within the national security field obtain 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 produced some undesirable results:

1. Technology vendors are deploying ECC schemes based on divergent standardization efforts or proprietary specifications that frustrate interoperability.
2. Technology vendors are avoiding deployment of the standardized techniques, thwarting the adoption and availability of commercial products.
3. New standardization efforts are 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 the IETF Memo entitled "Fundamental Elliptic Curve Cryptography Algorithms."[25]

---

[23] *See*, FIPS PUB 197 at the National Institute of Standards and Technology, FIPS Publications listing.

[24] *See*, http://www.nsa.gov/ia/contacts/index.shtml for more information.

[25] Available at http://tools.ietf.org/html/draft-mcgrew-fundamental-ecc-01.txt

Intellectual property rights (IPR) statements and frequently asked questions (FAQs) covering pricing have been made concerning some commercial use of patented ECC technology.[26] 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, as in the NSA Cryptographic Interoperability Strategy, have been highly effective in building multivendor 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.

4.1.3 Smart Grid System-Specific Encryption and Key Management Issues – Smart 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 the use of one secret key or a common credential across the entire infrastructure. Each device should have unique credentials or key material such that compromise of one device does not impact other deployed devices. The key management system (KMS) must also support an appropriate lifecycle of periodic rekeying 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 Advanced Metering Infrastructure (AMI) networks. Compromising a meter in one network could compromise all meters and collectors in both networks.

4.2 Cryptography and Key Management Solutions and Design Considerations

Secure key management is essential to the effective use of cryptography in deploying a Smart Grid infrastructure. NIST SP 800-57, *Recommendation for Key Management 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 they are a starting point for Smart Grid key management.[27]

4.2.1 General Design Considerations

4.2.1.1 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 cryptographic

[26] *See,* http://www.certicom.com/images/pdfs/certicom%20-ipr-contribution-to-ietfsept08.pdf and http://www.certicom.com/images/pdfs/certicom%20zigbee%20smart%20energy%20faq_30_mar_2009.pdf

[27] Please see Chapter 9 R&D for a discussion of some of the considerations.

community that openly-published and time-tested cryptographic algorithms and protocols are less likely to contain security flaws than those developed in secrecy, 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 the PE Mode as used in IEEE P1711 and EAX' as used in American National Standard (ANS) C12.22.

The general concerns are that these additional techniques have not 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 (1) be defined in a publicly available forum, (2) be provided to a community of cryptographers for review and comment for a reasonable duration, (3) be in, or under development in, a standard by a recognized standards-developing 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.

4.2.1.2 Entropy

As discussed earlier in the section there are considerations when dealing with entropy on many constrained devices and systems that can be found throughout the Smart Grid. There are some possible approaches that can address restricted sources of entropy on individual point devices, they include:

- Seeding a Deterministic Random Bit Generator (DRBG) on a device before distribution; any additional entropy produced within the device could be used to reseed it.
- Alternatively, a Key Derivation Function (KDF) could derive new keys from a long-term key that the device has been pre-provisioned with.

4.2.1.3 Cryptographic Module Upgradeability

Cryptographic algorithms are implemented within cryptographic modules that need to be designed to protect the cryptographic algorithm and keys used in the system. The following need to be considered when planning the upgradeability of these modules:

- Smart Grid equipment is often required to have an average life of 20 years, which is much longer than for typical information technology (IT) and communications systems.
- Due to reliability requirements for the electrical grid, testing cycles are often longer and more rigorous.
- The replacement of deployed devices can take longer and be more costly than for many IT and communications systems (e.g., wholesale replacement of millions of smart meters).

Careful consideration in the design and planning phase of any device and system for Smart Grid needs to take the above into account.

Over time, there have been challenges with obtaining and maintaining the required level of protection when using cryptographic algorithms, protocols, and their various compositions in working systems. For example, failures in encryption systems usually occur because of one or more of the following issues ranked, in order of decreasing likelihood:

- *Implementation errors*. Examples can include poor random number generator (RNG) seeding, poor sources of entropy, erroneous coding of a protocol/algorithm, HSM application program interface (API) errors/vulnerabilities that lead to Critical Security Parameter (CSP) leakage, etc.
- *Compositional failures*. Combining cryptographic algorithms without adequate analysis, which leads to less secure systems overall.
- *Insecure protocols*. This occurs when items, such as authentication protocols, are found to be insecure while their underlying algorithms may be secure. It is a similar issue to compositional failure, but protocols are inherently more complex constructions, as they usually involve multiparty message flows and possible complex states.
- *Insecure algorithms*. The probability that basic modern cryptographic algorithms, such as symmetric/asymmetric encryption and/or hash functions would become totally insecure is relatively low, but it always remains a possibility, as new breakthroughs occur in basic number theory, cryptanalysis, and new computing technologies. What is more likely is that subtle errors, patterns, or other mathematical results that reduce the theoretical strength of an algorithm will be discovered. There is also a long term (perhaps beyond the scope of many equipment lifetimes being deployed in Smart Grid) possibility of Quantum Computing (QC) being realized. The cryptographic consequences of QC vary, but current research dictates that the most relied upon asymmetric encryption systems (e.g. RSA, ECC, DH) would fail. However, doubling key sizes for symmetric ciphers (e.g. AES 128 bit to 256 bit) should be sufficient to maintain their current security levels under currently known theoretical attacks.

When designing and planning for Smart Grid systems, there are some design considerations that can address the risks under discussion:

- The use of approved and thoroughly reviewed cryptographic algorithms is strongly advised. The NIST Computer Security Division[28] has published a wealth of such cryptographic mechanisms and implementation guidance.
- Well-understood, mature, and publicly vetted methods that have been extensively peer-reviewed by a community of cryptographers and an open standards process should be preferred over cryptographic compositions or protocols that are based on proprietary and closed development.
- Independently validated cryptographic implementations, where cost and implementation feasibility allow, should be preferred over non-reviewed or unvalidated implementations.
- Cryptographic modules (both software and hardware) that can support algorithm and key length flexibility and maintain needed performance should be preferred over those that

[28] *See*, http://csrc.nist.gov.

cannot be changed, in case an algorithm is found to be no longer secure or a bit-strength-reducing vulnerability is found in the cryptographic algorithm.

- Providing a cryptographic design (including, but not limited to, key length) that exceeds current security requirements in order to avoid or delay the need for later upgrade.
- Cryptographic algorithms are often used within communications protocols. To enable possible future changes to the cryptographic algorithms without disrupting ongoing operation, it is good practice to design protocols that allow alternative cryptographic algorithms. Examples can include the negotiation of security parameters, such that future changes to cryptographic algorithms may be accommodated within the protocol (e.g., future modifications, with backwards compatibility), and support the simultaneous use of two or more cryptographic algorithms during a period of transition.
- It is understood that there will be cases in which, due to cost, chip specialization to particular standards, performance requirements, or other practical considerations, a cryptographic algorithm implementation (or aspects of it, such as key length) may not be upgradeable. In such cases, it may be prudent to ensure that adequate planning is in place to treat affected devices/systems as less trusted in the infrastructure and, for example, use enhanced network segmentation, monitoring, and containment (upon possible intrusion or tampering detection).

4.2.1.4 Random Number Generation

Random numbers or pseudorandom numbers are frequently needed when using cryptographic algorithms, e.g., for the generation of keys and challenge/responses in protocols. The failure of an underlying random number generator can lead to the compromise of the cryptographic algorithm or protocol and, therefore, the device or system in which the weakness appears.

Many Smart Grid devices may have limited sources of entropy that can serve as good sources of true randomness. The design of a secure random number generator from limited entropy is notoriously difficult. Therefore, the use of a well-designed, securely seeded and implemented deterministic random bit generator (i.e., also known as a pseudorandom number generator) is required. In some cases Smart Grid devices may need to include additional hardware to provide a good source of true random bits for seeding such generators.

There are several authoritative sources of information on algorithms to generate random numbers. One is NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)*. [§4.4-18]

Another source is the multi-part American National Standard (ANS) X9.82 Standard being developed within ASC X9. Part 1 is "Overview and Basic Principles," Part 2 is "Entropy Sources," Part 3 is "Deterministic Random Bit Generators (DRBGs)," and Part 4 is "Random Bit Generation Constructions." As of February 2010, only Parts 1 and 3, published in 2006 and 2007, respectively, are available as published standards. Note that Part 3 of ANS X9.82 contains three of the four DRBGs contained within NIST SP 800-90.

NIST and ANSI have been collaborating and continue to collaborate closely on this work.

NIST has also published NIST SP 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* [§4.4-11], which provides a comprehensive description of a battery of tests for RNGs that purport to provide non-biased

output. Both the report and the software may be obtained from http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html.

4.2.1.5 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.

4.2.1.6 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 find 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 permit the bypass or deauthorization of compromised devices (e.g., by revocation of the certificates of the compromised devices).

4.2.1.7 Algorithms and Key Lengths

NIST SP 800-57, *Recommendation for Key Management* [§4.4-15] recommends the cryptographic algorithms and key lengths to be used to attain given security strengths. Any KMS used in the Smart Grid should carefully consider these guidelines and provide rationale when deviating from these recommendations.

4.2.1.8 Physical Security Environment

The protection of Critical Security Parameters (CSPs), such as keying material and authentication data, is necessary to maintain the security provided by cryptography. To protect against unauthorized access, modification, or substitution of this data, as well as device tampering, cryptographic modules can include features that provide physical security.

There are multiple embodiments of cryptographic modules that may provide physical security, including: multichip standalone, multichip embedded, and single-chip devices. Specific examples of such device types providing cryptographic services and physical security include Tamper Resistant Security Modules (TRSMs), Hardware Security Modules, Security Authentication Module cards (SAM cards), which may have been validated as FIPS 140-2 cryptographic modules.

Physical protection is an important aspect of a module's ability to protect itself from unauthorized access to CSPs and tampering. A cryptographic module implemented in software and running on an unprotected system, such as a general-purpose computer, commonly does not have the ability to protect itself from physical attack. When discussing cryptographic modules, the term "firmware" is commonly used to denote the fixed, small, programs that internally

control a module. Such modules are commonly designed to include a range of physical security protections and levels.

In determining the appropriate level of physical protections required for a device, it is important to consider both the operating environment and the value and sensitivity of the data protected by the device. Therefore, the specification of cryptographic module physical protections is a management task in which both environmental hazard and data value are taken into consideration. For example, management may conclude that a module protecting low value information and deployed in an environment with physical protections and controls, such as equipment cages, locks, cameras, and security guards, etc., requires no additional physical protections and may be implemented in software executing on a general purpose computer system. However, in the same environment, cryptographic modules protecting high value or sensitive information, such as root keys, may require strong physical security.

In unprotected or lightly protected environments, it is common to deploy cryptographic modules with some form of physical security. Even at the consumer level, devices that process and contain valuable or sensitive personal information often include physical protection. Cable Television Set-top boxes, DVD players, gaming consoles, and smart cards are examples of consumer devices. Smart Grid equipment, such as smart meters, deployed in similar environments will, in some cases, process information and provide functionality that can be considered sensitive or valuable. In such cases, management responsible for meter functionality and security may determine that meters must include cryptographic modules with a level of physical protection.

In summary, cryptographic modules may be implemented in a range of physical forms, as well as in software on a general purpose computer. When deploying Smart Grid equipment employing cryptographic modules, the environment, the value of the information, and the functionality protected by the module should be considered when assessing the level of module physical security required.

4.2.2 Key Management Systems for Smart Grid

4.2.2.1 Public Key Infrastructure

4.2.2.1.1 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 of the certificate. As will be shown below, it is important to consider certificates as valid only 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 certification was issued to a device that was lost, stolen, or sent to a repair depot), the certificate can be revoked. Certificate revocation lists are used to store the certificate serial number and revocation date for all revoked certificates. An entity that bases its actions on the information in a certificate is called a Relying Party (RP). To determine if the RP can accept the certificate, the RP needs to check the following criteria, at a minimum:

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 RP's trust anchor) are being used between the notBefore and notAfter dates.
3. The certificates are not in an authoritative 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.

This section focuses primarily on steps 2 and 3.

4.2.2.1.2 Proper Use of Certificate Revocation, 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 certificates are added to the revocation list, (e.g., devices are replaced and no longer needed, but the certificate has not expired). 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 need no longer be kept on the CRL, 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 manageably-sized CRLs, against issuing certificates with longer validity periods and lower operational overhead, but with potentially large and unwieldy 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 certificate expiration date. In this way (by issuing relatively short life certificates), the CRLs can be kept to a reasonable size.

When certificates are issued to devices that are expected to last for many years, and these devices are housed in a secure environment, it may not be necessary to issue a 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 then arises: When a Smart Grid RP receives a certificate from an entity (person or device), and the certificate has 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, consider that Smart Grid devices will be deployed with the intent to keep them operational for many years (probably in the neighborhood of 10 to 15 years). Therefore, replacing these devices should not occur very often. Of course, there will be unplanned defects that will cause devices to be replaced from time to time. The certificates of these defective devices will need to be listed on the CRL when the devices are removed from service, unless their keys can be guaranteed to be securely destroyed. In order to avoid the unlimited growth of CRLs, it would be prudent to issue device certificates with an appropriate lifetime. For devices expected to last 20

years, which are housed in secure facilities, and have a low mean-time-before-failure (MTBF), a 10-year certificate may be appropriate. This means that when a device having a certificate of this length is installed in the system and subsequently fails, it 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 no longer be able to communicate in the system. To avoid this, the device could be provisioned with a "renewed" certificate quite some time before its current certificate expires. For example, the device may be provisioned with a new 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 to obtain a new certificate. It is therefore easy to see that the 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 with a new certificate sufficiently before the expiration of the old certificate."

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 the 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 for 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 allow CRLs to be fragmented into multiple files; or the use of 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 the efficient use of bandwidth; however they do nothing to keep the size of the CRLs reasonable.

4.2.2.1.3 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 technique 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 always be 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 communicate 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 its own signed certificate status and carries it with itself. When authenticating with an RP, the certificate subject not only provides its certificate, but also provides its 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. OCSP stapling offers a powerful, high-availability solution for determining a certificate's status.

4.2.2.1.4 Other Issues Relating to Certificate Status

A number of additional considerations with respect to certificate status issues are as follows:

- Smart Grid components may have certificates issued by their manufacturer. These certificates would indicate the manufacturer, model and serial number of the device. If so, Smart Grid operators (e.g., utility companies) 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 (i.e., the device) is owned by Utility Company X, it is installed in Substation Y, and is authorized to participate in Application Z. These certificates could be new identity certificates that 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 human roles change. For certificates issued to devices, identity certificates that include attributes may offer a lower cost solution.
- Standardized Trust Management mechanisms would include cross-signing procedures, policy constraints for cross-signed certificates, requirements for local and regional bridge providers, as well as approved methods for issuing temporary credentials to entities during incidents involving exceptional system outages. Ideally, such methods for issuing temporary credentials 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 the 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, 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 arrive 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 health care (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, all categories of devices, and specific requirements on the PKI participants for each supported assurance level. Furthermore, such standards could include accreditation criteria for Smart Grid PKI service providers.
- Additional thought needs to go into determining what 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. Furthermore, the device will need to use remote device attestation techniques to prove to others that it has not been tampered with.

- Some certificate subjects (i.e., devices or people) should have secure hardware for storing private keys and trust anchor certificates. Due to the advent of the Smart Card market, such mechanisms have become very affordable.
- RPs should have access to a reasonably accurate, trustworthy time source to determine if a certificate is being used within its validity period.
- Further consideration should go into determining appropriate certificate lifetimes.

4.2.2.1.5 Certificate Revocation List 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 20 ~1 kb partition files is feasible, compared to requesting and storing an "infinitely long" CRL.

The other alternative is the Online Certificate Status Protocol, which as the name implies, is an online, real-time service. OCSP is optimal in its space requirements, as the OCSP server 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, which simply sends back an "OK" or "BAD" indication. This approach requires no storage on the fielded device, but it does require the communications link to be active.

4.2.2.1.6 Trust Roots

A typical Web browser ships with a large number of built-in certificates (e.g., some modern browsers with up to 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 and load management services, it may not be appropriate for the utility company 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 is the certificate subject. 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 organizations, 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.

4.2.2.2 Single Sign On

Many Smart Grid components, such as wireless devices (e.g., AMI), are low-processing-power devices with wireless interface (e.g., Zigbee) and are often connected to the backhaul networks with low bandwidth links. These components are typically equipped with 4–12 kb of RAM and 64–256 kb of flash memory. The link characteristics can also vary, depending upon the wireless radio features, such as the sleeping or idle mode of operation. For example, the advanced metering system may periodically be awakened and synced with the network to save power, rather than remain always active. Additional device requirements include (1) the support of multi-hop networks using mesh topology (e.g., to extend the backhaul reach back), and (2) support of multiple link layer technologies.

Advanced meters can also be used for other purposes besides simple metering data. For example, ANS C12.22 [§4.4-21] allows using advanced meters peering via relay or concentrators. Other applications should be able to run simultaneously on a single meter. For security requirements, each application needs to be authenticated and needs to preserve the integrity of the data provided to the system (e.g., billing system). In such scenarios, the protocol overhead and performance must be optimized, and performance must be taken into account for these low-processing power components.

From a key management perspective, optimization on the amount of exchanges and the footprint to execute peer authentication, key establishment, key update, and key deletion have to be considered for each communication layer and protocol that is used by Smart Grid components that need to be secured. This can be achieved by introducing the notion of single sign-on (SSO) to Smart Grid components (e.g., smart meters) so that one execution of peer authentication between a Smart Grid component and an authentication server can generate keys for multiple protocols within the same communication layer or across multiple communication layers. In a typical use case scenario, a smart meter may perform network access authentication based on public-key cryptography that generates a root key from which encryption keys are derived to protect each application, as well as the link-layer connection. The advantage of this scheme is that the computationally intensive public-key operation is required only once to generate the root key.

For example, the Extensible Authentication Protocol (EAP) [§4.4-22] supports multiple authentication methods called EAP methods, and its key management framework [§4.4-23] defines a key hierarchy for the Extended Master Session Key (EMSK), from which Usage-Specific Root Keys (USRKs) are derived to bootstrap encryption keys for multiple usages [§4.4-24]. EAP therefore can be a basis of SSO for smart meters. RFC 5295 [§4.4-24] also defines the key naming rule for USRK.

4.2.2.3 Symmetric Key Management

Symmetric key environments—often referred to as secret key—use a single key to both apply cryptographic protection to data (e.g., encrypt) and process cryptographically protected data (e.g., decrypt). Thus, a single key must be shared between two or more entities that need to communicate. As with any cryptographic system, there are advantages and disadvantages to this type of system. Symmetric cipher systems, relative to asymmetric ciphers, handle large amounts of data more efficiently. Symmetric keys often have a shorter lifespan than asymmetric keys, because of the amount of data that is protected using a single key; limiting the amount of data that is protected by a symmetric key helps reduce the risk of compromise of both the key and

thee data. This poses important challenges in the management of these keys. The primary considerations encompassing symmetric key management includes key generation, key distribution, and key agility (i.e., the ability to change keys quickly when needed to protect different data).

The protection of the symmetric key is paramount in this type of system and is the greatest challenge in symmetric key system management. The generation of a symmetric key can essentially be accomplished in two ways: (1) locally, on the end device platform, or (2) remotely, at a single facility not physically attached to the end device platform. In the local generation scenario, a Diffie-Hellman key agreement process provides a good example for this style of generation. A simplistic description of Diffie-Hellman involves two parties that use private information known by each party and public information known by both parties to compute a symmetric key shared between the two parties. In this case, no outside influences are involved in key generation, only information known by the parties that wish to communicate is used. However, local key generation is not always possible, due to end device limitations, such as limited processor power and local memory constraints for storage of the values needed for computation.

In the remote generation scenario, the symmetric key is generated by one entity (e.g., a key server) and transported to one or more other entities (e.g. the end points that will use the key—the key consumer's device). Placement of the symmetric key into the end points can be accomplished using multiple methods that include preplaced keys or electronically distributed keys. In the preplaced method, the symmetric key is manually entered (i.e., physically loaded) into the key consuming device prior to the use of the key. This can be achieved at the factory or done when the device is deployed into the field. Electronically distributed keys need to be protected as they transit across the network to their destination. This can be achieved by encrypting the symmetric key so that only the end device can decrypt the key.

The remote generation scenario has more complexity associated with it because of distribution and trust risks. However, in the remote generation and distribution model, the concept of Perfect Forward Secrecy (PFS) can be managed for a large population of devices. PFS is dependent on the use of an ephemeral key, such that no previously used key is reused. In remote or central key generation and distribution models, PFS can be ensured because the key generation node can keep track of all previously used keys.

The preparation of the symmetric keys to be used needs to take into account both the organization (i.e., crypto groups) of which devices receive a given symmetric key and the set of keys for those devices that are needed to provide key agility. Thus, organizational management of symmetric key groups is critical to retaining control of the symmetric key as it is distributed.

Another area for consideration relative to physical key distribution is the method to establish the trust relationship between the end device and a key loader[29]—a topic beyond the scope of this section, but mentioned here for the sake of completeness. In actual practice, it will be necessary for the system managers to determine how this trust relationship is established. Establishing the

[29] A key loader is a device that is used to load keys directly into a device that performs encryption operations. A usage example would be in cases s where connectivity to the encryption platform has been lost and field personnel need to physically transport the keys to the encryption platform.

trust relationship should be based on a number of factors that focus on risks to the physical transport of the keys to the end point.

In the electronic distribution scenario where the symmetric key is generated by a key server that is external to the key consumer (i.e., the end point), the trust problem and the protection of the symmetric key in transit are paramount considerations to the successful implementation of this scenario. To mitigate the risk of disclosure, the key should be transported to the key consumer by wrapping (i.e., encrypting) the plaintext symmetric key, used for data protection, with a key encryption key (KEK). An individual KEK can be created by using the public key issued to the key consumer device. This way the symmetric key can be wrapped by the key generation server using the end devices public key and only unwrapped by the end devices private key. By using this method only the key consumer is able to extract the symmetric key, because only the key consumer has the associated private key, which of course remains protected on the key consumer's platform.

As can be seen, in symmetric key systems that distribute the operational key via an electronic method, a high level of coordination must be accomplished between the key producer and the key consumers. This means that a large amount of coordination management is levied on the key producer. Some considerations that the key producer must take into account include knowing exactly what group of key consumers receive the same symmetric key, risks to the key distribution channel, the key schedule to ensure that the key consumer has the right key at the right time, and how to recover from a key compromise. There are distinct advantages to remote key generation, especially since many of the devices in the Smart Grid may have limited resources, such as the processor power needed for key generation, physical memory to hold the algorithms to locally generate the symmetric key (e.g., random number generators), and the associated communications overhead to ensure that the proper key is used between the end points.

The final topic to discuss in symmetric key management is that of key agility. Key agility becomes critical when a compromise takes place as well as in normal operational mode and is directly related to preparation of the symmetric keys for use. In the case of a key compromise, key agility allows the key consumer to change to another key so that uninterrupted communication between end points can continue. However, key agility must be part of the overall key management function of planning and distribution. The key distribution package must also contain enough key material to provide operational keys plus have key material to support a compromise recovery. In the scenario where a compromise takes place, the compromise recovery key would be used, which would allow the key distribution point enough time to generate a new key package for distribution. Additionally the compromise recovery key may not be part of the same numerical branch as the previously used key to prevent a follow-on compromise where the attacker was able to determine the roll over key, based on the previously compromised key.

In the normal operational scenario where the key's lifetime comes to a natural end, the next key needs to be available to all key consumers within the same crypto group[30] prior to usage in order to ensure continuous communications. It should be noted that key roll over and the roll over

[30] A crypto group is a group of end devices that share a common symmetric key thereby creating a cryptographic group.

strategy is highly dependent on how the system uses the symmetric key and the frequency of communications using that key. Thus, in a scenario where communications is infrequent and the key distribution channel is secure, only a single key might be distributed to the consumer devices.

The ultimate decision on how to manage the symmetric key environment must rely on a risk assessment that considers such factors as key consumption frequency, the amount of data to be processed by the key, the security and capacity of the distribution channel, the number of symmetric keys required, and the methodology used to distribute the symmetric keys.

4.3 NISTIR HIGH-LEVEL REQUIREMENT MAPPINGS

4.3.1 Introduction

There is a need to specify cryptographic requirements and key management methods to be used in security protocols and systems that can fulfill the high-level CIA requirements. The source material that will be used to build these cryptographic requirements is in [§4.4-3] and [§4.4-4]. In summary, the high-level requirements (HLR) define low, moderate, and high levels for confidentiality, integrity, and availability, and each of these CIA requirements are mapped against the current 22 interface categories.

The interface categories are meant to capture the unique function and performance aspects of the classes of systems and devices in the Smart Grid. The cryptographic requirements that will be recommended, including those for key management, take into account the performance, reliability, computation, and communications attributes of systems and devices found in each interface category. In other words, best efforts where made to make sure that whatever is recommended should be technically and economically feasible and appropriate to the risk that must be addressed. The requirements mapping will be based on a framework for KMS attributes whose properties can be quantitatively and qualitatively analyzed for their application to the high-level requirements. Specifically, KMS attributes will be matched against the low, moderate, and high CIA levels. They will be the same for both Confidentiality and Integrity, since the capabilities and qualities of the KMS should default to the higher-level requirement in the case of cryptography. In terms of specific cryptographic suites of algorithms and key lengths, the cryptographic period requirements of NIST SP 800-57 should be used, as these requirements are not governed by anything to be found in the HLR, but by the intended lifetime of systems and their data or communication messages.

The framework of the mapping will consist of an identified cryptographic suite that is NIST-approved (i.e., FIPS-approved and/or NIST recommended) or allowed, as well as a KMS requirements matrix that maps to the HLR definitions of low, moderate, and high. The KMS matrix is a base-line for all the interface categories and can be adjusted for specific interface categories to take specific technical and risk based reasoning into account.

4.3.2 Framework

4.3.2.1 NIST-Approved Cipher Suite for Use in the Smart Grid

4.3.2.1.1 Introduction

Because Smart Grid devices can have a long operating life, the selection of cryptographic algorithms, key length, and key management methods should take into consideration the NIST transition dates specified in the following. This document lists all of the FIPS 140-2 Approved and allowed Security Functions, Random Number Generators, and Key Establishment Techniques as identified in FIPS 140-2 Annexes A, C, and D (as of 5/11/2010) and identifies which of these will be phased out by NIST as indicated in the following NIST documents:

- SP 800-57 [§4.4-15]
- SP 800-131, *DRAFT Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes* [§4.4-20]

It is important to note that the information provided in this document (i.e., NISTIR 7628) is based on the following:

- SP 800-131 is in Draft form. It is accounted for in this document because of the algorithm transition changes between 2011 and 2015. This document will be updated when the final version of SP 800-131 is released.
- The algorithms/key lengths in this document are relevant and important for NEW Implementations and those that will last beyond the year 2015. For existing implementations (i.e., validated FIPS modules), there is an expected "transition period that is provided in SP 800-131.

4.3.2.1.2 Background

All of the cryptographic algorithms that are required for use in the Smart Grid shall be NIST-approved as they currently exist today and as referenced in this report. During the development of updated versions of this report, a liaison shall be appointed to coordinate with NIST's Cryptographic Technology Group to ensure that any new algorithms are NIST-approved or allowed, and not scheduled to be withdrawn.

4.3.2.1.3 Rationale

The CSWG is chartered to coordinate cyber security standards for the Smart Grid. Since one of the primary goals is interoperability, the CSWG needs to ensure that any standards under consideration be usable by all stakeholders of the Smart Grid.

In the area of cryptography, federal law[31] requires that U.S. federal government entities must use NIST-approved or allowed algorithms. From FIPS-140-2: [§4.4-5]

> 7. Applicability. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the

[31] The Federal Information Security Management Act of 2002; the Information Technology Management Reform Act of 1996

> Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against this standard. The adoption and use of this standard is available to private and commercial organizations.

Given that many participants in the Smart Grid (including AMI) are U.S. federal agencies, interoperability requires that CSWG-listed standards be usable by them. Examples are the Tennessee Valley Authority, Bonneville Power Administration, and military bases around the world.[32]

Finally, a team of NIST cryptographers and the broader cryptographic community and general public, under a rigorous process, have reviewed the NIST-approved or allowed cryptographic suite. The goal of this robust process is to identify known weaknesses.

Examination of exceptions to the requirement:

The CSWG understands that there may exist standards and systems that take exception to this position on sound technical grounds and are potentially equally secure. The CSWG will consider these alternatives, based on submitted technical analysis that explains why the existing NIST-approved or allowed cryptographic suite could not be used. If the CSWG believes that the submitted technical analysis is sound, the CSWG will submit these other algorithms, modes, or any relevant cryptographic algorithms to NIST to be evaluated for approval for use in Smart Grid systems.

[32] A list of DOE-specific entities may be found at http://www.energy.gov/organization/powermarketingadmin.htm and http://www.energy.gov/organization/labs-techcenters.htm.

FIPS 140-2 Annex A: Approved Algorithms

Table 4-1 Symmetric Key – Approved Algorithms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
Advanced Encryption Standard (AES)	All algorithms/key lengths listed in the next column are Approved during this time.	AES-128, AES-192, and AES-256 with ECB, CBC, OFB, CFB-1, CFB-8, CFB-128, CTR, or XTS mode.	National Institute of Standards and Technology, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001. National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001. National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, Special Publication 800-38E, January 2010.
Triple-Data Encryption Algorithm (TDEA) or Triple-Data-Encryption-Standard (Triple-DES or TDES)	3-key TDES with TECB, TCBC, TCFB, TOFB, or CTR mode. (Note: 2-key TDES has 80 bits of security strength. All new implementations should have 112 bits of security strength or higher.)	N/A – cannot use TDES beyond 2030 (Note: 2-key TDES and 3-key TDES are not Approved because they have <128 bits of security.)	National Institute of Standards and Technology, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Special Publication 800-67, May 2004. National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001. Appendix E references Modes of Triple-DES.

Table 4-2 Asymetric Key – Approved Algortihms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
Digital Signature Standard (DSS): Digital Signature Algorithm (DSA) RSA digital signature algorithm (RSA) Elliptic Curve Digital Signature Algorithm (ECDSA)	DSA with (L=2048, N=224) or (L=2048, N=256) RSA with (|n|=2048) ECDSA2 with curves P-224, K-233, or B-233 Additionally, all algorithms/key lengths listed in the next column are Approved during this time. (Note: FIPS 186-2 algorithms should not be used because they are being phased out by NIST. DSA with (L=1024, N=160), RSA with (|n|=1024), and ECDSA curves K-163, B-163, P-192 have <112 bits of security.) All new implementations should have 112 bits of security strength or higher.)	DSA with (L=3072, N=256)** RSA with (|n|=3072)** ECDSA2 with curves P-256, P-384, P-521, K-283, K-409, K-571, B-283, B-409, B-571 **FIPS 186-3 recommends that the use of DSA with (L=3072, N=256) and RSA with (|n|=3072) should be limited to Certificate Authorities (CAs) (FIPS 186-3, Sections 4.2 and 5.1). (Note: FIPS 186-2 algorithms should not be used because they are being phased out by NIST. Key sizes less than those listed above are not Approved because they have <128 bits of security.)	National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-3, June, 2009. (DSA, RSA2 and ECDSA2) National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, January, 2000 with Change Notice 1. (DSA, RSA and ECDSA) RSA Laboratories, *PKCS#1 v2.1: RSA Cryptography Standard*, June 14, 2002. Only the versions of the algorithms RSASSA-PKCS1-v1_5 and RSASSA-PSS contained within this document shall be used.

Table 4-3 Secure Hash Standard (SHS) – Approved Algorithms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
Secure Hash Standard (SHS): Secure Hash Algorithm (SHA)	SHA-224 is Approved for all applications. Additionally, hash functions listed in the next column are Approved during this time.	SHA-256, SHA-384, and SHA-512 are Approved for all applications.	National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-3, October, 2008. (Note: FIPS 180-4 is expected to be released in the near future).

Table 4-4 Message Authentication – Approved Algortihms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
CMAC	CMAC with 3-key TDES Additionally, all algorithms/key lengths listed in the next column are Approved during this time. (Note: CMAC with 2-key TDES has 80 bits of security strength. All new implementations should have 112 bits of security strength or higher.)	CMAC with AES-128, AES-192, or AES-256 (Note: CMAC with TDES is not Approved because it has <128 bits of security.)	National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, Special Publication 800-38B, May 2005.
CCM	All algorithms/key sizes listed in the next column are Approved during this time.	CCM with AES-128, AES-192, or AES-256	National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, May

			2004.
GCM/GMAC	All algorithms/key sizes listed in the next column are Approved during this time.	GCM with AES-128, AES-192, or AES-256	National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Special Publication 800-38D, November 2007.
HMAC	HMAC with SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 with 112≤Key Length<128 bits Additionally, all algorithms/key sizes listed in the next column are Approved during this time. (Note: 2-key TDES has 80 bits of security strength. HMAC with Key Length <112 bits is should not be used because it is being phased out by NIST. All new implementations should have 112 bits of security strength or higher.)	HMAC with SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 with Key Length≥128 bits (Note: Any HMAC with Key Length <128 bits is not Approved because it has <128 bits of security.)	National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198, March 06, 2002

Table 4-5 Key Management – Approved Algortihms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
SP 800-108 KDFs	See rules for HMAC and CMAC; the PRFs used by the KDFs are based on these algorithms.	See rules for HMAC and CMAC; the PRFs used by the KDFs are based on these algorithms.	National Institute of Standards and Technology, *Recommendation for Key Derivation Using Pseudorandom Functions*, Special Publication 800-108, October 2009, Revised.

Table 4-6 Deterministic Random Number Generators – Approved Algorithms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
FIPS 186-2 Appendix 3.1 RNG	FIPS 186-2 RNG will be phased out by NIST by 2015. (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	N/A – cannot use FIPS 186-2 RNG (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, January 27, 2000 with Change Notice – Appendix 3.1.
FIPS 186-2 Appendix 3.2 RNG	FIPS 186-2 RNG will be phased out by NIST by 2015. (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	N/A – cannot use FIPS 186-2 RNG (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, January 27, 2000 with Change Notice – Appendix 3.2. Note: Please review National Institute of Standards and Technology, *Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program*, Sections 8.1, 8.7 and 8.9 for additional guidance.
ANSI X9.31-1998 Appendix A.2.4 RNG	ANSI X9.31 RNG will be phased out by NIST by 2015. (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	N/A – cannot use ANSI X9.31 RNG (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	American Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1998 - Appendix A.2.4.
ANSI X9.62-1998 Annex A.4 RNG	ANSI X9.62-1998 RNG will be phased out by NIST by 2015. (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	N/A – cannot use ANSI X9.62-1998 RNG (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	American Bankers Association, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, ANSI X9.62-1998 – Annex A.4.

ANSI X9.31 Appendix A.2.4 RNG using TDES and AES RNG	ANSI X9.31 RNG will be phased out by NIST by 2015. (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	N/A – cannot use ANSI X9.31 RNG (Note: The use of SP 800-90 RNGs is recommended since all other RNGs are being phased out by NIST.)	National Institute of Standards and Technology, *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms*, January 31, 2005.
SP 800-90 RNG	CTR DRBG with 3-key TDES is Approved. Additionally, all algorithms/key sizes listed in the next column are Approved during this time.	HASH DRBG with SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 HMAC DRBG with SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 CTR DRBG with AES-128, AES-192, or AES-256 DUAL EC DRBG with P-256, P-384, or P-521 (Note: CTR DRBG with 3-key TDES is not Approved because it has <128 bits of security.)	National Institute of Standards and Technology, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)*, Special Publication 800-90, March 2007.

Table 4-7 Non-Deterministic Random Number Generators – Algorithms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
Non-deterministic Random Number Generators	N/A – Currently none	N/A – Currently none	There are no FIPS Approved non-deterministic random number generators. Non-Approved RNGs may be used to seed Approved RNGs.

			(Note: The requirements for Non-deterministic and Non-Approved RNGs are still an open topic. CMVP guidance may change in 2015.)

Table 4-8 Symmetric Key Establishment Techniques – Approved Algortihms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
FIPS 140-2 IG D.2	3-key TDES Key Wrap *is* allowed. AES Key Wrap is Draft. (Note: 2-key TDES Key Wrap should not be used because it is being phased out by NIST. All new implementations should have 112 bits of security strength or higher.)	AES Key Wrap with 128-bit keys or higher *is* allowed. (Note: 3-key TDES Key Wrap is not allowed because it has <128 bits of security.	The symmetric key establishment techniques are listed in *FIPS 140-2 Implementation Guidance* Section D.2.

Table 4-9 Asymmetric Key Establishment Techniques – Approved Algortihms

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
SP 800-56A	Key Establishment with Parameter Sets FB, FC, and EB are Approved. Key Establishment using Diffie-Hellman is approved. Additionally, all algorithms/key sizes listed in the next column	Key Establishment with Parameter Sets EC, ED, and EE are Approved.	National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revision1)*, Special Publication 800-56A, March 2007.

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
	may be approved during this time. (Note: Parameter Sets FA and EA should not be used because they are being phased out by NIST. All new implementations should have 112 bits of security strength or higher.)	(Note: Parameter Sets FB, FC, and EB are not Approved because they have <128 bits of security.)	
SP 800-56B	Key Establishment using RSA-2048 for key transport/key agreement is Approved. (Note: RSA-1024 should not be used because it is being phased out by NIST. All new implementations should have 112 bits of security strength or higher.)	N/A – Cannot use RSA-2048 (Note: Use with RSA-2048 is not Approved because it has <128 bits of security.)	National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, Special Publication 800-56B, August 2009
FIPS 140-2 IG D.2	SP 800-56A primitives (using Parameter Sets FB, FC, and EB) with non-SP 800-56A KDFs in IG D.2 *are* allowed. Additionally, all algorithms/key sizes listed in the next column are allowed during this time. ***Important:*** These algorithms are only "allowed" in FIPS mode at this time. It is unclear if they will become Approved.	SP 800-56A primitives (using Parameter Sets EC, ED, and EE) with non-SP 800-56A KDFs in IG D.2 *are* allowed. ***Important:*** These algorithms are only "allowed" in FIPS mode at this time. It is unclear if	Additional asymmetric key establishment schemes are allowed in a FIPS Approved mode of operation. These schemes are listed with appropriate restrictions in *FIPS 140-2 Implementation Guidance* Section D.2.

Name	Algorithms/Key Lengths for use between 2011-2029 (per SP 800-57 and SP 800-131)	Algorithms/Key Lengths for use now and beyond 2030 (per SP 800-57 and SP 800-131)	References
	See IG D.2 for details. (Note: Parameter Sets FA and EA should not be used because they are being phased out by NIST. All new implementations should have 112 bits of security strength or higher.)	they will become Approved. See IG D.2 for details. (Note: Parameter Sets FB, FC, and EB are not allowed because they have <128 bits of security.)	

Table 4-10 Comparable Key Strengths

Bits of Security	Symmetric Key Algorithms	FCC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
80	2TDEA	L = 1024 N = 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N = 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N = 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	k = 15360	f ≥ 512

Table 4-11 Crypto Lifetimes[33]

Algorithm Security Lifetimes	Symmetric Key Algorithms (Encryption and MAC)	FCC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through December 31, 2013 (minimum of 80 bits of strength)	2TDEA[a] 3TDEA AES-128 AES-192 AES-256	$\|p\| = 1024$; $\|q\| = 160$[b] $\|p\| \geq 2048$; $\|q\| \geq 224$[c]	$1024 \leq \|n\| < 2048$[d] $\|n\| \geq 2048$[e]	$160 \leq \|n\| < 224$[b] $\|n\| \geq 224$[f]
Through December 31, 2030 (minimum of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min: L = 2048 N = 228	Min: k = 2048	Min: f = 224
Beyond 2030 (minimum of 128 bits of strength)	AES-128 AES-192 AES-256	Min: L = 3072 N = 256	Min: k = 3072	Min: f = 256

a Encryption: acceptable through 2010; restricted use from 2011-2015. Decryption: acceptable through 2010; legacy use after 2010.

b Digital signature generation and key agreement: acceptable through 2010; deprecated from 2011 through 2013. Digital signature verification: acceptable through 2010; legacy use after 2010.

c Digital signature generation and verification: acceptable. Key agreement: $|p|$=2048, and $|q|$=224 acceptable.

d Digital signature generation: acceptable through 2010; deprecated from 2011 through 2013. Digital signature verification: acceptable through 2010; legacy use after 2010. Key agreement and key transport: $|n|$=1024 acceptable through 2010, and deprecated from 2011 through 2013.

e Digital signature generation and verification: acceptable. Key agreement and key transport: $|n|$=2048 acceptable.

f Digital signature generation and verification, and key agreement: acceptable.

[33] *See* SP 800-131 for details.

Table 4-12 Hash Function Security Strengths

Bits of Security	Digital Signatures and Hash-Only Applications	HMAC	Key Derivation Functions	Random Number Generation
80	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
112	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
128	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
192	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
256	SHA-512	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512

4.3.3 KMS Requirements Matrix

4.3.3.1 Key Attribute Definitions

- **Key material and crypto operation protection:** A cryptography module's ability to protect its operational state from tampering and/or provide evidence of tampering. The module should also be able to keep its internal state private from general access. In the case of a Hardware Security Module (HSM), such protections are provided through physical hardware controls. In the case of software, such protection are limited and logical in nature, and may make use of some underlying hardware and operating system platform controls that offer memory protections, privileged execution states, tamper-detections, etc.
- **Key material uniqueness:** The KMS ensures that there is an adequate diversity of key material across the various devices and components participating in a system. For example, this is in order to protect against a compromise of one device such as a smart meter causing to a collapse of security in an entire system if all the keys are the same.
- **Key material generation:** The generation of key materials is secure and inline with established and known good methods, such as those listed in the NIST FIPS-140-2 standards.
- **Local autonomy:** All authentication processes between devices, or between users and devices will be able to operate even if a centralized service over a network is not available at any given time. For example, this is to ensure that if a network connection in a substation becomes unavailable, but a critical operation needs to be accomplished by local personnel, they would not in any way be inhibited from doing so.
- **Revocation management:** The ability to revoke credentials in a system in an ordered manner that ensures that all affected devices and users are notified and can take appropriate actions and adjustments to their configurations. Examples can include handling revoked PKI certificates and ensuring that entities with revoked certificates cannot be authenticated to protected services and functions.
- **Key material provisioning:** The processes and methods used to securely enter key material initially into components and devices of a system, as well as changing key materials during their operation.
- **Key material destruction:** The secure disposal of all key material after its intended use and lifetime, for example, the zeriozation / erasure of CSPs. Making key material unavailable is an acceptable alternative for systems where destruction is not possible.
- **Credential span of control:** The number of organizations, domains, systems or entities controlled or controllable through the use of the key material associated with the credential. This does not explicitly address keys used for purposes other than control nor include asymmetric keys that are indirectly used for control, such as those associated with root or intermediate certification authorities.

4.3.3.2 General Definitions

- **Hardware Security Module (HSM):** A module that provides tamper evidence/proofing, as well as the protection of all critical security parameters (CSPs) and cryptographic processes from the systems they operate in such that they can never be accessed in plaintext outside of the module.
- **Root of security:** A credential/secret or aggregation point of credentials such that there is a catastrophic loss of trust if compromised. Alternatively, root(s) of hierarchical trust credentials.

4.3.3.3 KMS Requirements

Table 4-13 KMS Requirements

Attribute	Low	Moderate	High	Requirements	Reference
Key material and cryptographic operations protection		X	X	Software protection of cryptographic materials used in individual devices (e.g. control system devices)	FIPS 140-2 Level 1
			X	Hardware protection (such as HSM) for Critical Security Parameters (CSPs) for Roots of security. It is recommended where possible to use FIPS-140-2 Level 2 or above for Physical Security.	FIPS 140-2 Levels 2 through 4
				Note: • *Symmetric and Asymmetric Keys used for authorization shall be protected from generation until the end of the cryptoperiod.* • *The integrity of all keys used for authorization must be protected. The confidentiality of Private and Symmetric keys must be protected.*	
Key material uniqueness, (e.g., key derivation secrets, managing secrets, pre-shared secrets)		X	X	Key diversity is required for High-assurance devices (unique keys per device (asymmetric) or device pairs (symmetric). This is to ensure that a single compromise of a device cannot lead to a complete collapse of security of the entire system.	NIST SP 800-57, Section 5.2
		X	X	All root key material shall be unique (with the exception of derived materials).	
Key material generation	X	X	X	Use Approved methods.	FIPS 140-2, Section 4.7.2 Annex C: Approved Random Number Generators for FIPS PUB 140-2
	X	X	X	NIST-approved RNGs need to be used.	FIPS 140-2, Section 4.7.2

Attribute	Low	Moderate	High	Requirements	Reference
					Annex C: Approved Random Number Generators for FIPS PUB 140-2
				Note: There is some concern that there needs to be non-NIST approved RNG to address the lack of entropy available to some SG devices. *FIPS allows the use of non-deterministic RNGs to produce entropy. Pre-loading entropy is also acceptable.}*	
Local autonomy (Availability Exclusively)		X	X	Must always be locally autonomous. That is no authentication process must depend on a centralized service such that if it were to become unavailable local access would not be possible.	
Revocation management	X	X	X	A credential revocation process must be established whereby all parties relying on a revoked key are informed of the revocation with complete identification of the keying material, and information that allows a proper response to the revocation.	NIST SP 800-57, Section 8.3.5
			X	Near real time/real time revocation (for example: a push based mechanism)	
Key material provisioning			X	Key distribution shall be performed in accordance with sp 800-57 (ref section 8.1.5.2.2) • Keys distributed manually (i.e., by other than an electronic key transport protocol) shall be protected throughout the distribution process. • During manual distribution, secret or private keys shall either be encrypted or be distributed using appropriate physical security procedures. o The distribution shall be from an authorized source, o Any entity distribution plaintext keys is trusted by both the entity that generates the keys and the entity(ies) that receives the keys,	NIST SP 800-57, Section 8.1.5.2.2 FIPS 140-2, Sections 4.7.3 and 4.7.4

Attribute	Low	Moderate	High	Requirements	Reference
				o The keys are protected in accordance with Section 6 [800-57], and o The keys are received by the authorized recipient.	
	X	X	X	Keys entered over a network interface must be encrypted (not for trusted roots). *Note: This is defined for operational provisioning of a system. That is manufacture time key material is provisioned that is a bootstrap for user/owner based provisioning.*	FIPS 140-2, Section 4.7.4
			X	The manual entry of plaintext keys or key components must be performed over a trusted interface. (e.g. a dedicated, physical point to point connection to an HSM) for some higher assurance modules it will also require split or encrypted key entry.	FIPS 140-2, Section 4.7.4
Key material Destruction		X	X	All copies of the private or symmetric key shall be destroyed as soon as no longer required (e.g., for archival or reconstruction activity).	SP 800-57, Section 8.3.4
		X	X	Any media on which unencrypted keying material requiring confidentiality protection is stored shall be erased in a manner that removed all traces of the keying material so that it cannot be recovered by either physical or electronic means	SP 800-57, Section 8.3.4 FIPS 140-2, Section 4.7.6
				Note: If key destruction needs to be assured, then an HSM must be used. Zeroization applies to an operational environment and does not apply to keys that may be archived.	SP 800-57, Section 8.3.4
Key and crypto lifecycles (supersession / revocation)	X	X	X	NIST recommended cryptoperiods shall be used (SP 800-57, table 1 provides a summary) *Note: Mechanism used to replace a key must have at least the same crypto strength as the key it is replacing.*	SP 800-57, Table 1
				Note: Cryptoperiod. The requirement will be to follow SP 800-57 Key management requirements. Supersession:	

Attribute	Low	Moderate	High	Requirements	Reference
				process of creating the next key and moving to that key and getting rid of old key.	
Credential span of control		X	X	The span of control for asymmetric keys shall in general be limited to a domain or a set of contiguous domains under the control of a single legal entity such as a systems operator. Exceptions to this requirement MAY include: Root and Intermediate CAs servicing multi-system consortia where a common identity or credentialing system is required. *Note: For symmetric keys, the requirement for a single pair of systems is due to the underlying requirement that the compromise of one entity should not give you control over other entities (that you didn't already have). For asymmetric keys, the underlying requirement is to be able to have a finite space in which the revocations need to be distributed.*	
		X	X	A symmetric key shall not be used for control of more than a single entity.	

4.4 REFERENCES & SOURCES

1. NISTIR 7628, Draft 2: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628Feb2010
2. Bottom Up Cyber Security Analysis of Smart Grid, latest version from http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGBottomUp
3. High-level requirements collection: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGHighLevelRequirements
4. NIST Smart Grid Architecture materials: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGArchi
5. FIPS 140-2, *Security Requirements for Cryptographic Modules*
6. FIPS 180-3, *Secure Hash Standard (SHS)*
7. FIPS 186-3, *Digital Signature Standard (DSS)*
8. FIPS 197, *Advanced Encryption Standard (AES)*
9. FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*
10. NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*
11. NIST SP 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*
12. NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*
13. NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*
14. NIST SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*
15. NIST SP 800-57, *Recommendation for Key Management*
16. NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*
17. NIST SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*
18. NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
19. NIST SP 800-102, *Recommendation for Digital Signature Timeliness*
20. SP 800-131, *DRAFT Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes*
21. American National Standard Institute, "Meter and End Device Tables communications over any network", ANSI C12.22-2008, 2008.
22. B. Aboba, et al., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

23. "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, August 2008.

24. J. Salowey, et al., "Specification for the Derivation of Root Key from an Extended Master Session Key (EMSK)", RFC 5295, August 2008.

25. National Security Agency, Suite B Cryptography, http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

APPENDIX A
CROSSWALK OF CYBER SECURITY DOCUMENTS

Table A-1 Crosswalk of Cyber Security Requirements and Documents

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
Access Control (SG.AC)						
SG.AC-1	Access Control Policy and Procedures	AC-1	Access Control Policy and Procedures	2.15.1	Access Control Policies and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)
SG.AC-2	Remote Access Policy and Procedures	AC-17	Remote Access	2.15.23	Remote Access Policy and Procedures	CIP005-2 (R1, R1.1, R1.2, R2, R2.3, R2.4)
SG.AC-3	Account Management	AC-2	Account Management	2.15.3	Account Management	CIP 003-2 (R5, R5.1, R5.2, R5.3) CIP 004-2 (R4, R4.1, R4.2) CIP 005-2 (R2.5) CIP 007-2 (R5, R5.1, R5.2)
SG.AC-4	Access Enforcement	AC-3	Access Enforcement	2.15.7	Access Enforcement	CIP 004-2 (R4) CIP 005-2 (R2, R2.1-R2.4)
SG.AC-5	Information Flow Enforcement	AC-4	Information Flow Enforcement	2.15.15	Information Flow Enforcement	
SG.AC-6	Separation of Duties	AC-5	Separation of Duties	2.15.8	Separation of Duties	
SG.AC-7	Least Privilege	AC-6	Least Privilege	2.15.9	Least Privilege	CIP 007-2 (R5.1)
SG.AC-8	Unsuccessful Login Attempts	AC-7	Unsuccessful Login Attempts	2.15.20	Unsuccessful Logon Notification	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.AC-9	Smart Grid Information System Use Notification	AC-8	System Use Notification	2.15.17	System Use Notification	CIP 005-2 (R2.6)
SG.AC-10	Previous Logon Notification	AC-9	Previous Logon (Access) Notification	2.15.19	Previous Logon Notification	
SG.AC-11	Concurrent Session Control	AC-10	Concurrent Session Control	2.15.18	Concurrent Session Control	
SG.AC-12	Session Lock	AC-11	Session Lock	2.15.21	Session Lock	
SG.AC-13	Remote Session Termination			2.15.22	Remote Session Termination	
SG.AC-14	Permitted Actions without Identification or Authentication	AC-14	Permitted Actions without Identification or Authentication	2.15.11	Permitted Actions without Identification and Authentication	
SG.AC-15	Remote Access	AC-17	Remote Access	2.15.24	Remote Access	CIP 005-2 (R2, R3, R3.1, R3.2)
SG.AC-16	Wireless Access Restrictions			2.15.26	Wireless Access Restrictions	
SG.AC-17	Access Control for Portable and Mobile Devices	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)
SG.AC-18	Use of External Information Control Systems	SC-7	Boundary Protection	2.15.29	Use of External Information Control Systems	
SG.AC-19	Control System Access Restrictions			2.15.28	External Access Protections	
SG.AC-20	Publicly Accessible Content					
SG.AC-21	Passwords			2.15.16	Passwords	CIP 007-2 (R5.3)
Awareness and Training (SG.AT)						

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.AT-1	Awareness and Training Policy and Procedures	AT-1	Security Awareness and Training Policy and Procedures	2.11.1	Security Awareness Training Policy and Procedures	CIP 004-2 (R1, R2)
SG.AT-2	Security Awareness	AT-2	Security Awareness	2.11.2	Security Awareness	CIP 004-2 (R1)
SG.AT-3	Security Training	AT-3	Security Training	2.11.3	Security Training	CIP 004-2 (R2)
SG.AT-4	Security Awareness and Training Records	AT-4	Security Training Records	2.11.4	Security Training Records	CIP 004-2 (R2.3)
SG.AT-5	Contact with Security Groups and Associations	AT-5	Contact with Security Groups and Associations	2.11.5	Contact with Security Groups and Associations	
SG.AT-6	Security Responsibility Training			2.11.6	Security Responsibility Training	
SG.AT-7	Planning Process Training			2.7.5	Planning Process Training	CIP 004-2 (R2)
Audit and Accountability (SG.AU)						
SG.AU-1	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)
SG.AU-2	Auditable Events	AU-2	Auditable Events	2.16.2	Auditable Events	CIP 005-2 (R1, R1.1, R1.3) CIP 007-2 (R5.1.2, R5.2.3, R6.1, R6.3)
		AU-13	Monitoring for Information Disclosure			
SG.AU-3	Content of Audit Records	AU-3	Content of Audit Records	2.16.3	Content of Audit Records	CIP 007-3 (R5.1.2)
SG.AU-4	Audit Storage Capacity	AU-4	Audit Storage Capacity	2.16.4	Audit Storage	

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) May 2009
SG.AU-5	Response to Audit Processing Failures	AU-5	Response to Audit Processing Failures	2.16.5	Response to Audit Processing Failures	
SG.AU-6	Audit Monitoring, Analysis, and Reporting	AU-6	Audit Monitoring, Analysis, and Reporting	2.16.6	Audit Monitoring, Process, and Reporting	CIP 007-2 (R5.1.2) CIP 007-2 (R6.5)
SG.AU-7	Audit Reduction and Report Generation	AU-7	Audit Reduction and Report Generation	2.16.7	Audit Reduction and Report Generation	
SG.AU-8	Time Stamps	AU-8	Time Stamps	2.16.8	Time Stamps	
SG.AU-9	Protection of Audit Information	AU-9	Protection of Audit Information	2.16.9	Protection of Audit Information	CIP 003-2 (R4)
SG.AU-10	Audit Record Retention	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 (R2)
SG.AU-11	Conduct and Frequency of Audits	AU-1	Audit and Accountability Policy and Procedures	2.16.11	Conduct and Frequency of Audits	
SG.AU-12	Auditor Qualification			2.16.12	Auditor Qualification	
SG.AU-13	Audit Tools	AU-7	Audit Reduction and Report Generation	2.16.13	Audit Tools	
SG.AU-14	Security Policy Compliance	CA-1	Security Assessment and Authorization Policies and Procedures	2.16.14	Security Policy Compliance	
SG.AU-15	Audit Generation	AU-12	Audit Generation	2.16.15	Audit Generation	
SG.AU-16	Non-Repudiation	AU-10	Non-Repudiation	2.16.16	Non-Repudiation	
Security Assessment and Authorization (SG.CA)						

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.CA-1	Security Assessment and Authorization Policy and Procedures	CA-1	Security Assessment and Authorization Policies and Procedures	2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures	
				2.17.1	Monitoring and Reviewing Control System Security management Policy and Procedures	
SG.CA-2	Security Assessments	CA-2	Security Assessments	2.17.3	Monitoring of Security Policy	
SG.CA-3	Continuous Improvement			2.17.2	Continuous Improvement	
				2.17.4	Best Practices	
SG.CA-4	Information System Connections	CA-3	Information System Connection	2.18.5	Control System Connections	CIP 005-2 (R2)
SG.CA-5	Security Authorization to Operate	CA-6	Security Authorization	2.17.5	Security Accreditation	
		PM-10	Security Authorization Process			
SG.CA-6	Continuous Monitoring	CA-7	Continuous Monitoring	2.18.7	Continuous Monitoring	
Configuration Management (SG.CM)						
SG.CM-1	Configuration Management Policy and Procedures	CM-1	Configuration Management Policy and Procedures	2.6.1	Configuration Management Policy and Procedures	CIP 003-2 (R6)
SG.CM-2	Baseline Configuration	CM-2	Baseline Configuration	2.6.2	Baseline Configuration	CIP 007-2 (R9)
SG.CM-3	Configuration Change Control	CM-3	Configuration Change Control	2.6.3	Configuration Change Control	CIP 003-2 (R6)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
		SA-10	Developer Configuration Management			
SG.CM-4	Monitoring Configuration Changes	CM-4 SA-10	Security Impact Analysis Developer Configuration Management	2.6.4	Monitoring Configuration Changes	CIP 003-2 (R6)
SG.CM-5	Access Restrictions for Configuration Change	CM-5	Access Restrictions for Change	2.6.5	Access Restrictions for Configuration Change	CIP 003-2 (R6)
SG.CM-6	Configuration Settings	CM-6	Configuration Settings	2.6.6	Configuration Settings	CIP 003-2 (R6) CIP 005 (R2.2)
SG.CM-7	Configuration for Least Functionality	CM-7	Least Functionality	2.6.7	Configuration for Least Functionality	
SG.CM-8	Component Inventory	CM-8	Information System Component Inventory	2.6.8	Configuration Assets	
SG.CM-9	Addition, Removal, and Disposal of Equipment	MP-6	Media Sanitization	2.6.9	Addition, Removal, and Disposition of Equipment	CIP 003-2 (R6)
SG.CM-10	Factory Default Settings Management			2.6.10	Factory Default Authentication Management	CIP 005-2 (R4.4)
SG.CM-11	Configuration Management Plan	CM-9	Configuration Management Plan			
Continuity of Operations (SG.CP)						
SG.CP-1	Continuity of Operations Policy and Procedures	CP-1	Contingency Planning Policy and Procedures			

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.CP-2	Continuity of Operations Plan	CP-1	Contingency Planning Policy and Procedures	2.12.2	Continuity of Operations Plan	CIP 008-2 (R1) CIP 009-2 (R1)
SG.CP-3	Continuity of Operations Roles and Responsibilities	CP-2	Contingency Plan	2.12.3	Continuity of Operations Roles and Responsibilities	CIP 009-2 (R1.1, R1.2)
SG.CP-4	Continuity of Operations Training					
SG.CP-5	Continuity of Operations Plan Testing	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)
SG.CP-6	Continuity of Operations Plan Update			2.12.6	Continuity of Operations Plan Update	CIP 009-2 (R4, R5)
SG.CP-7	Alternate Storage Sites	CP-6	Alternate Storage Sites	2.12.13	Alternative Storage Sites	
SG.CP-8	Alternate Telecommunication Services	CP-8	Telecommunications Services	2.12.14	Alternate Command/Control Methods	
SG.CP-9	Alternate Control Center	CP-7 CP-8	Alternate Processing Site Telecommunications Services	2.12.15	Alternate Control Center	
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	CP-10	Information System Recovery and Reconstitution	2.12.17	Control System Recovery and Reconstitution	CIP 009-2 (R4)
SG.CP-11	Fail-Safe Response			2.12.18	Fail-Safe Response	
Identification and Authentication (SG.IA)						
SG.IA-1	Identification and Authentication Policy	IA-1	Identification and Authentication Policy and	2.15.2	Identification and Authentication	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
	and Procedures		Procedures		Procedures and Policy	
SG.IA-2	Identifier Management	IA-4	Identifier Management	2.15.4	Identifier Management	
SG.IA-3	Authenticator Management	IA-5	Authenticator Management	2.15.5	Authenticator Management	CIP 007-2 (R5, R5.1, R5.2, R5.3)
SG.IA-4	User Identification and Authentication	IA-2	User Identification and Authentication	2.15.10	User Identification and Authentication	CIP 003-2 (R1, R1.1, R1.3)
SG.IA-5	Device Identification and Authentication	IA-3	Device Identification and Authentication	2.15.12	Device Authentication and Identification	
SG.IA-6	Authenticator Feedback	IA-6	Authenticator Feedback	2.15.13	Authenticator Feedback	
Information and Document Management (SG.ID)						
SG.ID-1	Information and Document Management Policy and Procedures			2.9.1	Information and Document Management Policy and Procedures	
SG.ID-2	Information and Document Retention			2.9.2	Information and Document Retention	CIP 006-2 (R7)
SG.ID-3	Information Handling	MP-1	Media Protection Policy and Procedures	2.9.3	Information Handling	CIP 003-2 (R4.1)
SG.ID-4	Information Exchange			2.9.5	Information Exchange	
SG.ID-5	Automated Labeling			2.9.11	Automated Labeling	
Incident Response (SG.IR)						
SG.IR-1	Incident Response Policy and Procedures	IR-1	Incident Response Policy and Procedures	2.12.1	Incident Response Policy and Procedures	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.IR-2	Incident Response Roles and Responsibilities	IR-1	Incident Response Policy and Procedures	2.7.4	Roles and Responsibilities	CIP 008-2 (Rr1.2) CIP 009-2 (R1.2)
SG.IR-3	Incident Response Training	IR-2	Incident Response Training	2.12.4	Incident Response Training	
SG.IR-4	Incident Response Testing and Exercises	IR-3	Incident Response Testing and Exercises			
SG.IR-5	Incident Handling	IR-4	Incident Handling	2.12.7	Incident Handling	
SG.IR-6	Incident Monitoring	IR-5	Incident Monitoring	2.12.8	Incident Monitoring	
SG.IR-7	Incident Reporting	IR-6	Incident Reporting	2.12.9	Incident Reporting	
SG.IR-8	Incident Response Investigation and Analysis	PE-6	Monitoring Physical Access	2.12.11	Incident Response Investigation and Analysis	CIP 008-2 (R1, R1.2-R1.5)
SG.IR-9	Corrective Action			2.12.12	Corrective Action	CIP 008-2 (R1.4) CIP 009-2 (R3)
SG.IR-10	Smart Grid Information System Backup	CP-9	Information System Backup	2.12.16	Control System Backup	
SG.IR-11	Coordination of Emergency Response			2.2.4	Coordination of Threat Mitigation	CIP 008-2 (R1.3)
Smart Grid Information System Development and Maintenance (SG.MA)						
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	MA-1	System Maintenance Policy and Procedures	2.10.1	System Maintenance Policy and Procedures	
SG.MA-2	Legacy Smart Grid Information System Updates			2.10.2	Legacy System Upgrades	

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) May 2009
SG.MA-3	Smart Grid Information System Maintenance	PL-6	Security-Related Activity Planning	2.10.5	Unplanned System Maintenance	
		MA-2	Controlled Maintenance	2.10.6	Periodic System Maintenance	
SG.MA-4	Maintenance Tools	MA-3	Maintenance Tools	2.10.7	Maintenance Tools	
SG.MA-5	Maintenance Personnel	MA-5	Maintenance Personnel	2.10.8	Maintenance Personnel	
SG.MA-6	Remote Maintenance	MA-4	Non-Local Maintenance	2.10.9	Remote Maintenance	
SG.MA-7	Timely Maintenance	MA-6	Timely Maintenance	2.10.10	Timely Maintenance	CIP 009-2 (R4)
Media Protection (SG.MP)						
SG.MP-1	Media Protection Policy and Procedures	MP-1	Media Protection Policy and Procedures	2.13.1	Media Protection and Procedures	
SG.MP-2	Media Sensitivity Level	RA-2	Security Categorization	2.13.3	Media Classification	CIP 003-2 (R4, R4.2)
				2.9.4	Information Classification	
SG.MP-3	Media Marketing	MP-3	Media Marketing	2.13.4	Media Labeling	
				2.9.10	Automated Marking	
SG.MP-4	Media Storage	MP-4	Media Storage	2.13.5	Media Storage	
SG.MP-5	Media Transport	MP-5	Media Transport	2.13.6	Media Transport	
SG.MP-6	Media Sanitization and Disposal	MP-6	Media Sanitization	2.13.7	Media Sanitization and Storage	CIP 007-2 (R7, R7.1, R7.2, R7.3)
Physical and Environmental Security (SG.PE)						
SG.PE-1	Physical and Environmental Security Policy and Procedures	PE-1	Physical and Environmental Protection Policy and Procedures	2.4.1	Physical and Environmental Security Policies and Procedures	CIP 006-2 (R1, R2)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.PE-2	Physical Access Authorizations	PE-2	Physical Access Authorizations	2.4.2	Physical Access Authorizations	CIP 004-2 (R4)
SG.PE-3	Physical Access	PE-3	Physical Access Control	2.4.3	Physical Access Control	CIP 006-2 (R2)
		PE-4	Access Control for Transmission Medium			
		PE-5	Access Control for Output Devices			
SG.PE-4	Monitoring Physical Access	PE-6	Monitoring Physical Access	2.4.4	Monitoring Physical Access	CIP 006-2 (R5)
SG.PE-5	Visitor Control	PE-7	Visitor Control	2.4.5	Visitor Control	CIP 006-2 (R1.4)
SG.PE-6	Visitor Records	PE-8	Access Records	2.4.6	Visitor Records	CIP 006-2 (R1.4, R6)
SG.PE-7	Physical Access Log Retention			2.4.7	Physical Access Log Retention	CIP 006-2 (R7)
SG.PE-8	Emergency Shutoff Protection	PE-10	Emergency Shutoff	2.4.8	Emergency Shutoff	
SG.PE-9	Emergency Power	PE-11	Emergency Power	2.4.9	Emergency Power	
SG.PE-10	Delivery and Removal	PE-16	Delivery and Removal	2.4.14	Delivery and Removal	
SG.PE-11	Alternate Work Site	PE-17	Alternate Work Site	2.4.15	Alternate Work Site	
SG.PE-12	Location of Smart Grid Information System Assets	PE-18	Location of Information System Components	2.4.18	Location of Control System Assets	
Planning (SG.PL)						
SG.PL-1	Strategic Planning Policy and Procedures	PL-1	Security Planning and Procedures	2.7.1	Strategic Planning Policy and Procedures	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.PL-2	Smart Grid Information System Security Plan	PL-2	System Security Plan	2.7.2	Control System Security Plan	
SG.PL-3	Rules of Behavior	PL-4	Rules of Behavior	2.7.11	Rules of Behavior	
SG.PL-4	Privacy Impact Assessment	PL-5	Privacy Impact Assessment			
SG.PL-5	Security-Related Activity Planning	PL-6	Security-Related Activity Planning	2.7.12	Security-Related Activity Planning	CIP 002-2 (R1)
Security Program Management (SG.PM)						
SG.PM-1	Security Policy and Procedures	AC-1	Access Control Policy and Procedures	2.1.1	Security Policies and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)
SG.PM-2	Security Program Plan	PM-1	Information Security Program Plan			
SG.PM-3	Senior Management Authority	PM-2	Senior Information Security Officer			
SG.PM-4	Security Architecture	PM-7	Enterprise Architecture			
SG.PM-5	Risk Management Strategy	PM-9	Risk Management Strategy			
SG.PM-6	Security Authorization to Operate Process	PM-10	Security Authorization Process			
SG.PM-7	Mission/Business Process Definition	PM-11	Mission/Business Process Definition			
SG.PM-8	Management Accountability	PM-1	Information Security Program Plan	2.2.2	Management Accountability	CIP 003-2 (R2, R3)
Personnel Security (SG.PS)						

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.PS-1	Personnel Security Policy and Procedures	PS-1	Personnel Security Policy and Procedures	2.3.1	Personnel Security Policies and Procedures	CIP 004-2 (R3)
SG.PS-2	Position Categorization	PS-2	Position Categorization	2.3.2	Position Categorization	CIP 004-2 (R3)
SG.PS-3	Personnel Screening	PS-3	Personnel Screening	2.3.3	Personnel Screening	CIP 004-2 (R3)
SG.PS-4	Personnel Termination	PS-4	Personnel Termination	2.3.4	Personnel Termination	CIP 004-2 (R4.2) CIP 004-2 (R5.2.3)
SG.PS-5	Personnel Transfer	PS-5	Personnel Transfer	2.3.5	Personnel Transfer	CIP 004-2 (R4.1, R4.2)
SG.PS-6	Access Agreements	PS-6	Access Agreements	2.3.6	Access Agreements	
SG.PS-7	Contractor and Third-Party Personnel Security	PS-7	Third-Party Personnel Security	2.3.7	Third-Party Security Agreements	CIP 004-2 (R3.3)
SG.PS-8	Personnel Accountability	PS-8	Personnel Sanctions	2.3.8	Personnel Accountability	
SG.PS-9	Personnel Roles			2.3.9	Personnel Roles	
Risk Management and Assessment (SG.RA)						
SG.RA-1	Risk Assessment Policy and Procedures	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, R4.2)
SG.RA-2	Risk Management Plan	PM-9	Risk Management Strategy	2.18.2	Risk Management Plan	CIP 003-2 (R4, R4.1, R4.2)
SG.RA-3	Security Impact Level	RA-2	Security Categorization	2.18.8	Security Categorization	
SG.RA-4	Risk Assessment	RA-3	Risk Assessment	2.18.9	Risk Assessment	CIP 002-2 (R1.2)
SG.RA-5	Risk Assessment Update	RA-3	Risk Assessment	2.18.10	Risk Assessment Update	CIP 002-2 (R4)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.RA-6	Vulnerability Assessment and Awareness	RA-5	Vulnerability Scanning	2.18.11	Vulnerability Assessment and Awareness	CIP 005-2 (R4, R4.2, R4.3, R4.4) CIP 007-2 (R8)
Smart Grid Information System and Services Acquisition (SG.SA)						
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	SA-1	System and Services Acquisition Policy and Procedures	2.5.1	System and Services Acquisition Policy and Procedures	
SG.SA-2	Security Policies for Contractors and Third Parties			2.2.5	Security Policies for Third Parties	
				2.2.6	Termination of Third-Party Access	
SG.SA-3	Life-Cycle Support	SA-3	Life-Cycle Support	2.5.3	Life-Cycle Support	
SG.SA-4	Acquisitions	SA-4	Acquisitions	2.5.4	Acquisitions	
SG.SA-5	Smart Grid Information System Documentation	SA-5	Information System Documentation	2.5.5	Control System Documentation	
SG.SA-6	Software License Usage Restrictions	SA-6	Software Usage Restrictions	2.5.6	Software License Usage Restrictions	
SG.SA-7	User-Installed Software	SA-7	User-Installed Software	2.5.7	User-installed Software	
SG.SA-8	Security Engineering Principles	SA-8 SA-13	Security Engineering Principles	2.5.8	Security Engineering Principals	
			Trustworthiness			
SG.SA-9	Developer Configuration Management	SA-10	Developer Configuration Management	2.5.10	Vendor Configuration Management	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.SA-10	Developer Security Testing	SA-11	Developer Security Testing	2.5.11	Vendor Security Testing	
SG.SA-11	Supply Chain Protection	SA-12	Supply Chain Protection	2.5.12	Vendor Life-cycle Practices	
Smart Grid Information System and Communication Protection (SG.SC)						
SG.SC-1	System and Communication Protection Policy and Procedures	SC-1	System and Communication Protection Policy and Procedures	2.8.1	System and Communication Protection Policy and Procedures	CIP 003-2 (R1, R1.1, R1.3)
SG.SC-2	Communications Partitioning			2.8.2	Management Port Partitioning	
SG.SC-3	Security Function Isolation	SC-3	Security Function Isolation	2.8.3	Security Function Isolation	
SG.SC-4	Information Remnants	SC-4	Information in Shared Resources	2.8.4	Information Remnants	
SG.SC-5	Denial-of-Service Protection	SC-5	Denial-of-Service Protection	2.8.5	Denial-of-Service Protection	
SG.SC-6	Resource Priority	SC-6	Resource Priority	2.8.6	Resource Priority	
SG.SC-7	Boundary Protection	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)
SG.SC-8	Communication Integrity	SC-8	Transmission Integrity	2.8.8	Communication Integrity	
SG.SC-9	Communication Confidentiality	SC-9	Transmission Confidentiality	2.8.9	Communication Confidentially	
SG.SC-10	Trusted Path	SC-11	Trusted Path	2.8.10	Trusted Path	
SG.SC-11	Cryptographic Key Establishment and Management	SC-12	Cryptographic Key Establishment and Management	2.8.11	Cryptographic Key Establishment and Management	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.SC-12	Use of Validated Cryptography	SC-13	Use of Cryptography	2.8.12	Use of Validated Cryptography	
SG.SC-13	Collaborative Computing	SC-15	Collaborative Computing Devices	2.8.13	Collaborative Computing	
SG.SC-14	Transmission of Security Parameters	SC-16	Transmission of Security Attributes	2.8.14	Transmission of Security Parameters	
SG.SC-15	Public Key Infrastructure Certificates	SC-17	Public Key Infrastructure Certificates	2.8.15	Public Key Infrastructure Certificates	
SG.SC-16	Mobile Code	SC-18	Mobile Code	2.8.16	Mobile Code	
SG.SC-17	Voice-Over Internet Protocol	SC-19	Voice Over Internet Protocol	2.8.17	Voice-over-Internet Protocol	
SG.SC-18	System Connections	CA-3	Information System Connections	2.8.18	System Connections	CIP 005-2 (R2, R2.2-R2.4)
SG.SC-19	Security Roles	SA-9	External Information System Services	2.8.19	Security Roles	CIP 003-2 (R5)
SG.SC-20	Message Authenticity	SC-8	Transmission Integrity	2.8.20	Message Authenticity	
SG.SC-21	Secure Name/Address Resolution Service	SC-20	Secure Name/Address Resolution Service (Authoritative Source)	2.8.22	Secure Name/Address Resolution Service (Authoritative Source)	
SG.SC-22	Fail in Known State	SC-24	Fail in Known State	2.8.24	Fail in Know State	
SG.SC-23	Thin Nodes	SC-25	Thin Nodes	2.8.25	Thin Nodes	
SG.SC-24	Honeypots	SC-26	Honeypots	2.8.26	Honeypots	
SG.SC-25	Operating System-Independent Applications	SC-27	Operating System-Independent Applications	2.8.27	Operating System-Independent Applications	
SG.SC-26	Confidentiality of Information at Rest	SC-28	Confidentiality of Information at Rest	2.8.28	Confidentiality of Information at Rest	
SG.SC-27	Heterogeneity	SC-29	Heterogeneity	2.8.29	Heterogeneity	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
SG.SC-28	Virtualization Technique	SC-30	Virtualization Technique	2.8.30	Virtualization Techniques	
SG.SC-29	Application Partitioning			2.8.32	Application Partitioning	
SG.SC-30	Information System Partitioning	SC-32	Information Systems Partitioning			
Smart Grid Information System and Information Integrity (SG.SI)						
SG.SI-1	System and Information Integrity Policy and Procedures	SI-1	System and Information Integrity Policy and Procedures	2.14.1	System and Information Integrity Policy and Procedures	
SG.SI-2	Flaw Remediation	SI-2	Flaw Remediation	2.14.2	Flaw Remediation	CIP 007-2 (R3, R3.1, R3.2)
SG.SI-3	Malicious Code and Spam Protection	SI-3	Malicious Code Protection	2.14.3	Malicious Code Protection	CIP 007-2 (R4, R4.1, R4.2)
		SI-8	Spam Protection	2.14.8	Spam Protection	CIP 007-2 (R4)
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	SI-4	Information System Monitoring	2.14.4	System Monitoring Tools and Techniques	CIP 007-2 (R6)
SG.SI-5	Security Alerts and Advisories	SI-5	Security Alerts, Advisories, and Directives	2.14.5	Security Alerts and Advisories	
SG.SI-6	Security Functionality Verification	SI-6	Security Functionality Verification	2.14.6	Security Functionality Verification	CIP 007-2 (R1)
SG.SI-7	Software and Information Integrity	SI-7	Software and Information Integrity	2.14.7	Software and Information Integrity	
SG.SI-8	Information Input Validation	SI-10	Information Input Validation	2.14.9	Information Input Restrictions	CIP 003-2 (R5) CIP 007-2 (R, R5.1, R5.2)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
Smart Grid Cyber Security Requirement		**NIST SP 800-53 Revision 3**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) May 2009**
				2.14.10	Information Input Accuracy, Completeness, Validity and Authenticity	
SG.SI-9	Error Handling	SI-11	Error Handling	2.14.11	Error Handling	

APPENDIX B
EXAMPLE SECURITY TECHNOLOGIES AND SERVICES TO MEET THE HIGH-LEVEL 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, and 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 powerflow-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 powerflow-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.

Following are existing power system capabilities and features that may address the cyber security requirements included in this report. These existing capabilities may need to be tailored or expanded to meet the security requirements.

B.1 POWER SYSTEM CONFIGURATIONS AND ENGINEERING STRATEGIES

- Networked transmission grid so the loss of a single power system element will not cause a transmission outage (n-1 contingency),

- Redundant[34] power system equipment (e.g., redundant transmission lines, redundant transformers),
- Redundant information sources (e.g., redundant sensors, voltage measurements from different substation equipment or from different substations),
- Redundant communication networks (e.g., fiber optic network and power line carrier between substations, or redundant communication "headends"),
- Redundant automation systems (e.g., redundant substation protective relays, redundant SCADA computers systems, backup systems that can be quickly switched in),
- Redundant or backup control centers (e.g., SCADA systems in physically different locations),
- Redundant power system configurations (e.g., networked grids, multiple feeds to customer site from different substations),
- Redundant logs and databases with mirrored or frequent updates,
- Multiple generators connected at different locations on the transmission grid,
- Reserve generation capacity available to handle the loss of a generator,
- Configuration setting development procedures, including remedial relay settings, and
- Post-event engineering forensic analysis.

B.2 LOCAL EQUIPMENT MONITORING, ANALYSIS, AND CONTROL

- Sensors on substation and feeder equipment monitor volts, VARs, current, temperature, vibrations, etc. – eyes and ears for monitoring the power system,
- Control capabilities for local control, either automatically (e.g., breaker trip) or manually (e.g., substation technician raises the voltage setting on a tap changer),
- Voltage/VAR regulation by local equipment to ensure voltages and VARs remain within prescribed limits,
- Protective relaying to respond to system events (e.g., power system fault) by tripping breakers,
- Reclosers which reconnect after a "temporary" fault by trying to close the breaker 2-3 times before accepting it as a "permanent" fault,
- Manual or automatic switching to reconfigure the power system in a timely manner by isolating the faulted section, then reconnecting the unfaulted sections,
- Device event logs,
- Digital fault recorders,

[34] Redundancy is multiple instances of the same software, firmware, devices, and/or data configured in an active/passive or load sharing mode. Redundancy for data and logs needs to be consistent with the organization's data retention plan and continuity of operations plan.

- Power quality (PQ) harmonics recorders, and
- Time synchronization to the appropriate accuracy and precision.

B.3 CENTRALIZED MONITORING AND CONTROL

- SCADA systems have approximately 99.98% availability with 24x7 monitoring,
- SCADA systems continuously monitor generators, substations, and feeder equipment (e.g., every second and/or report status and measurements "by exception"),
- SCADA systems perform remote control actions on generators, substations, and feeder equipment in response to operator commands or software application commands,
- Automatic Generation Control (AGC) issues control commands to generators to maintain frequency and other parameters within limits,
- Load Shedding commands can drop feeders, substations, or other large loads rapidly in case of emergencies,
- Load Control commands can "request" or command many smaller loads to turn off or cycle off,
- Disturbance analysis (rapid snapshots of power system during a disturbance for future analysis),
- Alarm processing, with categorization of high priority alarms, "intelligent" alarm processing to determine the true cause of the alarm, and events, and
- Comparisons of device settings against baseline settings.

B.4 CENTRALIZED POWER SYSTEM ANALYSIS AND CONTROL

Energy Management Systems (EMS) and Distribution Management Systems (DMS) use many software functions to analyze the real-time state and probable future state of the power system. These software functions include:

- "Power Flow" models of the transmission system, generators, and loads simulate the real-time or future (or past) power system scenarios,
- "Power Flow" models of the distribution system simulate real-time or future power system scenarios,
- State estimation uses redundant measurements from the field to "clean up" or estimate the real measurements from sometimes noisy, missing, or inaccurate sensor data,
- Power flow applications use the state estimated data to better simulate real-time conditions,
- Load and renewable generation forecasts based on weather, history, day-type, and other parameters forecast the generation requirements,
- Contingency Analysis (Security Analysis) assesses the power flow model for single points of failure (n-1) as well as any linked types of failures, and flags possible problems,

- Generation reserve capacity is available for instantaneous, short term, and longer term supply of generation in the event of the loss of generation,
- Ancillary services from bulk generation are available to handle both efficiency and emergency situations (e.g. generator is set to "follow load" for improved efficiency, generator is capable of a "black start" namely to start up during an outage without needing external power),
- Fault Location, Isolation, and Service Restoration (FLISR) analyze fault information in real-time to determine what feeder section to isolate and how to best restore power to unfaulted sections,
- Volt/VAR/Watt Optimization determine the optimal voltage, VAR, and generation levels usually for efficiency, but also to handle contingencies and emergency situations,
- Direct control of DER and loads (load management) for both efficiency and reliability,
- Indirect control of DER and loads (demand response) for both efficiency and reliability, and
- Ancillary services from DER for both efficiency and reliability (e.g., var support from inverters, managed charging rates for PEVs).

B.5 TESTING

- Lab and field testing of all power system and automation equipment minimizes failure rates,
- Software system factory, field, and availability testing,
- Rollback capability for database updates,
- Configuration testing,
- Relay coordination testing, and
- Communication network testing, including near power system faults.

B.6 TRAINING

- Dispatcher training simulator, using snapshots of real events as well as scenarios set up by trainers,
- Operational training using case studies, etc.,
- Training in using new technologies, and
- Security training.

B.7 EXAMPLE SECURITY TECHNOLOGY AND SERVICES

The selection and implementation of security technology and services is based on an organization's specification of security requirements and analysis of risk. This process is outside the scope of this report. Included below are some example security technologies and services that are provided as guidance. These are listed with some of the Smart Grid common technical

requirements. The example security technologies and services for the unique technical requirements are included in the logical architectural diagrams included in this section.

Table B-2 Example Security Technologies and Services

Smart Grid Security Requirement	Smart Grid Requirement Name	Example Security Technologies/Services
SG.SC-15	Public Key Infrastructure Certificates	• Cryptographic and key management support • Secure remote certificate enrollment protocol, with appropriate cert policies matching authorization policies
SG.SC-16	Mobile Code	• Software quality assurance program ("the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle and that the software functions in the intended manner."["National Information Assurance Glossary"; CNSS Instruction No. 4009 National Information Assurance Glossary]) • Code inspection • Code-signing and verification on all mobile code • Allowed / Denied entities technology to detect mobile-code
SG.SC-18	System Connections	• Identification and authorization • Information classification • Security domains and network segmentation • Allowed / Denied entities services • Allowed / Denied entities connections
SG.SC-19	Security Roles	• Security management (data, attributes, functions, management roles, separation of duties) • Policy decision point (PDP) and Policy Enforcement Point (PEP) products • Role based access control (RBAC) • Training
SG.SC-20	Message Authenticity	• Non-repudiation of origin • Non-repudiation of receipt • Message integrity
SG.SC-21	Secure Name/Address Resolution Service	• Redundant name services • Restricting transaction entities based on IP address
SG.SC-22	Fail in Known State	• Fail secure • Trusted recovery at the firmware and system levels • Software quality assurance program
SG.SC-30	Information System Partitioning	• Traffic labeling and enforcement • Information classification program • Process (and Inter-process) access verification • Network-based and physical separation, labeling, etc. • RBAC technologies • Firewalls • OS-based process execution separation
SG.SI-8	Information Input	• User data protection

Smart Grid Security Requirement	Smart Grid Requirement Name	Example Security Technologies/Services
	Validation	• Internal system data protection • RBAC • Separation of duties • Software quality assurance program • Internal system data protection • Non-repudiation • Authentication • Data transfer integrity • Before processing any input coming from a user, data source, component, or data service it should be validated for type, length, and/or range • Implement transaction signing • Access controls must check that users are allowed to use an action before performing the rendering or action
SG.SI-9	Error Handling	• Log management program • Delivery of error messages over secure channel • Software quality assurance program
SG.AC-6	Separation of Duties	• Security management (data, attributes, functions, management roles, separation of duties) • RBAC • Training
SG.AC-7	Least Privilege	• Security management (data, attributes, functions, management roles, separation of duties) • RBAC • Security domains and network segmentation • Traffic classification and priority routing
SG.AC-21	Passwords	• Authentication • Identification • Subject binding • Password Complexity Enforcement • Salted Hashes • Password Cracking Tests
SG.AC-9	System Use Notification	• System access history • Logon banner or message
SG.AC-8	Unsuccessful Login Attempts	• Authentication failure notice • Logon banner or message • Failed Login Attempt Lockouts
SG.AC-17	Access Control for Portable and Mobile Devices	• Limitation on scope of selectable attributes • Limitation on multiple concurrent sessions • System access banners • System access history • Limitation of network access • Secure communications tunnel • Authentication
SG.AC-16	Wireless Access	• Limitation on scope of selectable attributes

Smart Grid Security Requirement	Smart Grid Requirement Name	Example Security Technologies/Services
	Restrictions	• Limitation on multiple concurrent sessions • System access banners • System access history • Limitation of network access • Secure communications tunnel • Authentication
SG.AU-2	Auditable Events	• Event logging standard • Log management program • Scalable log filtering/parsing • Centralize logging/syslog to a NOC or SOC • 7x24 real-time auditing and automatic event notification
SG.AU-3	Content of Audit Records	• Event logging standard • Security audit event selection • Security audit review and analysis • Log management program • Scalable log filtering/parsing • Centralize logging/syslog to a NOC or SOC • 7x24 real-time auditing and automatic event notification
SG.AU-4	Audit Storage Capacity	• Record retention standards and requirements • Regular archiving and management of logs • Centralize logs to an enterprise log management system • Enable automatic file system checks for available disk space • Log management program
SG.AU-15	Audit Generation	• Security audit automatic response • Security audit automatic data generation • Verify that application level auditing is implemented in COTS and custom code • Verify that OS level auditing exists • Centralize logging/syslog to a NOC or SOC

NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid

The Smart Grid Interoperability Panel – Cyber Security Working Group

August 2010

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

NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid

The Smart Grid Interoperability Panel–Cyber Security Working Group

August 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 (IT). 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 National Institute of Standards and Technology Interagency Report (NISTIR) 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, vol. 2
69 **pages (August 2010)**

ACKNOWLEDGMENTS

This report was developed by members of the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP-CSWG), formerly the Cyber Security Coordination Task Group (CSCTG), and during its development was chaired by Annabelle Lee of the Federal Energy Regulatory Commission (FERC), formerly of NIST. The CSWG is now chaired by Marianne Swanson (NIST). Alan Greenberg (Boeing), Dave Dalva (CiscoSystems), and Bill Hunteman (Department of Energy) are the vice chairs. Mark Enstrom (Neustar) is the secretary. Tanya Brewer of NIST is the lead editor of this report. The members of the SGIP-CSWG have extensive technical expertise and knowledge to address the cyber security needs of the Smart Grid. The dedication and commitment of all these individuals over the past year and a half is significant. In addition, appreciation is extended to the various organizations that have committed these resources to supporting this endeavor. Members of the SGIP-CSWG and the working groups of the SGIP-CSWG are listed in Appendix J of this report.

In addition, acknowledgement is extended to the NIST Smart Grid Team, consisting of staff in the NIST Smart Grid Office and several of NIST's Laboratories. Under the leadership of Dr. George Arnold, National Coordinator for Smart Grid Interoperability, their ongoing contribution and support of the CSWG efforts have been instrumental to the success of this report.

Additional thanks are extended to Diana Johnson (Boeing) and Liz Lennon (NIST) for their superb technical editing of this report. Their expertise, patience, and dedication were critical in producing a quality report. Thanks are also extended to Victoria Yan (Booz Allen Hamilton). Her enthusiasm and willingness to jump in with both feet are really appreciated.

Finally, acknowledgment is extended to all the other individuals who have contributed their time and knowledge to ensure this report addresses the security needs of the Smart Grid.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

OVERVIEW AND REPORT ORGANIZATION

REPORT OVERVIEW

Version 1.0 (V1.0) of NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, is the Smart Grid Interoperability Panel—Cyber Security Working Group's (SGIP-CSWG's) report for individuals and organizations who will be addressing cyber security for Smart Grid systems. This includes, for example, vendors, manufacturers, utilities, system operators, researchers, and network specialists; and individuals and organizations representing the IT, telecommunications, and electric sectors. This report assumes readers have a functional knowledge of the electric sector and a functional understanding of cyber security.

AUDIENCE

This report is intended for a variety of organizations that may have overlapping and different perspectives and objectives for the Smart Grid. For example—

- *Utilities/asset owners/service providers* may use this report as guidance for a specific Smart Grid information system implementation;
- *Industry/Smart Grid vendors* may base product design and development, and implementation techniques on the guidance included in this report;
- *Academia* may identify research and development topics based on gaps in technical areas related to the functional, reliability, security, and scalability requirements of the Smart Grid; and
- *Regulators/policy makers* may use this report as guidance to inform decisions and positions, ensuring that they are aligned with appropriate power system and cyber security needs.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
  - 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* includes a high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. The chapter also includes individual diagrams for each of the 22 logical interface categories. This architecture focuses on a short-term view (1–3 years) of the Smart Grid.
  - Chapter 3 – *High Level Security Requirements* specifies the high level security requirements for the Smart Grid for each of the 22 logical interface categories included in Chapter 2.

  - Chapter 4 – *Cryptography and Key Management* identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.
  - Appendix A – *Crosswalk of Cyber Security Documents*
  - Appendix B – *Example Security Technologies and Procedures to Meet the High Level Security Requirements*
- Volume 2 – Privacy and the Smart Grid
  - Chapter 5 – *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 that may occur as new capabilities are included in the Smart Grid.
  - Appendix C – *State Laws – Smart Grid and Electricity Delivery*
  - Appendix D – *Privacy Use Cases*
  - Appendix E – *Privacy Related Definitions*
- Volume 3 – Supportive Analyses and References
  - Chapter 6 – *Vulnerability Classes* includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.
  - Chapter 7 – *Bottom-Up Security Analysis of the Smart Grid* identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.
  - Chapter 8 – *Research and Development Themes for Cyber Security in the Smart Grid* 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.
  - Chapter 9 – *Overview of the Standards Review* includes an overview of the process that is being used to assess standards against the high level security requirements included in this report.
  - Chapter 10 – *Key Power System Use Cases for Security Requirements* identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.
  - Appendix F – *Logical Architecture and Interfaces of the Smart Grid*
  - Appendix G – *Analysis Matrix of Interface Categories*
  - Appendix H – *Mappings to the High Level Security Requirements*
  - Appendix I – *Glossary and Acronyms*
  - Appendix J – *SGIP-CSWG Membership*

CHAPTER FIVE
PRIVACY AND THE SMART GRID

The Smart Grid is an evolving construct of new technologies, services, and entities integrating with legacy solutions and organizations. The SGIP-CSWG privacy subgroup views the privacy chapter as a starting point for continuing the work to improve upon privacy practices as the Smart Grid continues to evolve and as new privacy threats, vulnerabilities and the associated risks emerge. The information in this chapter was developed as a consensus document by a diverse subgroup consisting of representatives from the privacy, electric energy, telecommunications and cyber industry, academia, and government organizations. The chapter does not represent legal opinions, but rather was developed to explore privacy concerns, and provide associated recommendations for addressing them. Privacy impacts and implications may change as the Smart Grid expands and matures. It should be noted that this chapter addresses residential users and their data. The CSWG Privacy Subgroup will begin to explore privacy concerns for commercial, industrial, and institutional energy consumers, and deliver updates to existing work to address any new privacy considerations based on the pace of Smart Grid evolution.

CHAPTER ABSTRACT

The Smart Grid brings with it many new data collection, communication, and information sharing capabilities related to energy usage, and these technologies in turn introduce concerns about privacy. *Privacy* relates to individuals. Four dimensions of privacy are considered: (1) *personal information*— any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, locational or social identity; (2) *personal privacy*—the right to control the integrity of one's own body; (3) *behavioral privacy*—the right of individuals to make their own choices about what they do and to keep certain personal behaviors from being shared with others; and (4) *personal communications privacy*—the right to communicate without undue surveillance, monitoring, or censorship.

Most Smart Grid entities directly address the first dimension, because privacy of personal information is what most data protection laws and regulations cover. However, the other three dimensions are important privacy considerations as well and should be considered by Smart Grid entities.

When considering how existing laws may deal with privacy issues within the Smart Grid, and likewise the potential influence of other laws that explicitly apply to the Smart Grid, it is important to note that while Smart Grid privacy concerns may not be expressly addressed, existing laws and regulations may still be applicable. Nevertheless, the innovative technologies of the Smart Grid pose new issues for protecting consumers' privacy that will have to be tackled by law or by other means.

The Smart Grid will greatly expand the amount of data that can be monitored, collected, aggregated, and analyzed. This expanded information, particularly from energy consumers and other individuals, raises added privacy concerns. For example, specific appliances and generators can be identified from the signatures they exhibit in electric information at the meter when collections occur with great frequency as opposed to through traditional monthly meter readings. This more detailed information expands the possibility of intruding on consumers' and other individuals' privacy expectations.

The research behind the material presented in this chapter focused on privacy within personal dwellings and electric vehicles and did not address business premises and the privacy of individuals within such premises. The researchers' conclusions based upon work in these primary areas are as follows:

- Evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, and their behavior within their premises and electric vehicles privacy risks and challenges that have not been tested and may or may not be mitigated by existing laws and regulations.

- New Smart Grid technologies, and particularly smart meters, smart appliances, and similar types of endpoints, create new privacy risks and concerns that may not be addressed adequately by the existing business policies and practices of utilities and third-party Smart Grid providers.

- Utilities and third-party Smart Grid providers need to follow standard privacy and information security practices to effectively and consistently safeguard the privacy of personal information.

- Most consumers probably do not understand their privacy exposures or their options for mitigating those exposures within the Smart Grid.

Based on initial research and the details of the associated findings, a summary listing of all recommendations includes the following points for entities that participate within the Smart Grid:

- Conduct pre-installation processes and activities for using Smart Grid technologies with utmost transparency.
- Conduct an initial privacy impact assessment before making the decision to deploy and/or participate in the Smart Grid. Additional privacy impact assessments should be conducted following significant organizational, systems, applications, or legal changes—and particularly, following privacy breaches and information security incidents involving personal information, as an alternative, or in addition, to an independent audit.

- Develop and document privacy policies and practices that are drawn from the full set of Organisation for Economic Cooperation and Development (OECD) Privacy Principles and other authorities (see 5.4.1 "Consumer-to-Utility PIA Basis and Methodology"). This should include appointing personnel responsible for ensuring

privacy policies and protections are implemented.

- Provide regular privacy training and ongoing awareness communications and activities to all workers who have access to personal information within the Smart Grid.
- Develop privacy use cases that track data flows containing personal information to address and mitigate common privacy risks that exist for business processes within the Smart Grid.
- Educate consumers and other individuals about the privacy risks within the Smart Grid and what they can do to mitigate them.
- Share information with other Smart Grid market participants concerning solutions to common privacy-related risks.

Additionally, manufacturers and vendors of smart meters, smart appliances, and other types of smart devices, should engineer these devices to collect only the data necessary for the purposes of the smart device operations. The defaults for the collected data should be established to use and share the data only as necessary to allow the device to function as advertised and for the purpose(s) agreed to by Smart Grid consumers.

5.1 INTRODUCTION

Modernizing the current electric grid through the computerization and networking of intelligent components holds the promise of a Smart Grid infrastructure that can—

- Deliver electricity more efficiently;
- Provide better power quality;
- Link with a wide array of energy sources in addition to energy produced by power plants (such as renewable energy sources);
- Enable self-healing in cases of disturbance, physical and cyber attack, or natural disaster; and
- Provide consumers, and other individuals[1], with more choices based on how, when, and how much electricity they use.

Communications technology that enables the bidirectional flow of information throughout the infrastructure is at the core of these Smart Grid improvements, which rely upon collated energy usage data provided by smart meters, sensors, computer systems, and many other devices to

[1] Because consumers are often thought of as the individuals who actually pay the energy bills, the SGIP-CSWG privacy group determined it was important to include reference all individuals who would be within a particular dwelling or location since their activities could also be determined in the ways described within this chapter. From this point forward, for brevity, only the term "consumers" will be used, but it will mean all the individuals applicable to the situation being described.

derive understandable and actionable information for consumers and utilities—and it is this same technology that also brings with it an array of privacy challenges. The granularity, or depth and breadth of detail, captured in the information collected and the interconnections created by the Smart Grid are factors that contribute most to these new privacy concerns.

The Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP-CSWG) has worked since June 2009 to research privacy issues within the existing and planned Smart Grid environment. Its research to date has focused on privacy concerns related to consumers' personal dwellings and use of electric vehicles.[2] In July and August of 2009, the privacy subgroup performed a comprehensive privacy impact assessment (PIA) for the consumer-to-utility portion of the Smart Grid, and the results of this study have enabled the group to make the recommendations found in this chapter for managing the identified privacy risks.

The privacy subgroup membership is derived from a wide range of organizations and industries, including utilities, state utility commissions, privacy advocacy groups, academia, Smart Grid appliance and applications vendors, information technology (IT) engineers, and information security (IS) practitioners. This diversity of disciplines and areas of interest among the group's participants helps to ensure all viewpoints are considered when looking at privacy issues, and it brought a breadth of expertise both in recognizing inherent privacy risk areas and in identifying feasible ways in which those risks might be mitigated while at the same time supporting and maintaining the value and benefits of the Smart Grid.

Because this chapter will be read by individuals with a wide range of interests, professional fields, and levels of expertise with respect to Smart Grid privacy issues, careful consideration has been given to the chapter's structure, which is as follows:

1. **Discussion of the concept of privacy**. This establishes our common ground in understanding the notion of "privacy," and defines the notion of privacy, where readers may hold different viewpoints on the subject.
2. **Definitions of privacy terms**. Privacy terms are defined differently among various industries, groups, countries, and even individuals. We define the privacy terms used in this chapter.
3. **Overview of current data protection laws and regulations with respect to privacy**. Even though numerous laws exist to establish a range of privacy protections, it is important to consider how those privacy protections apply to the Smart Grid.
4. **Determination of personal activities within the Smart Grid**. This explains the creation of new data types in the Smart Grid, as well as new uses for data that has formerly only been in the possession of utilities outside of retail access states.[3]

[2] There may also be privacy concerns for individuals within business premises, such as hotels, hospitals, and office buildings, in addition to privacy concerns for transmitting Smart Grid data across country borders. However, because the existing collection of NIST use cases does not cover business locations or cross border data transmission, and in view of its time constraints, the Privacy Group did not research business premises or cross border privacy issues. The Privacy Group recommends these as topics for further investigation.

[3] "Retail access states" refers to those states offering programs whereby energy services companies may supply service to customers at market-based prices.

5. **Summary of the consumer-to-utility PIA**. Identifies key privacy issues identified by the privacy subgroup in performing its PIA for the consumer-to-utility portion of the Smart Grid and provides a guide for subsequent research.
6. **In-depth look at privacy issues and concerns**. Addresses follow-on research based on the PIA findings in which the privacy subgroup explored the broader privacy issues that exist within the entire expanse of the Smart Grid.
7. **Detailed analysis of representative privacy use cases**. Use cases can help Smart Grid architects and engineers build privacy protections into the Smart Grid. Some example privacy use cases were created for specific scenarios within the Smart Grid to identify privacy concerns and demonstrate how to use privacy use cases. Developers of Smart Grid applications, systems, and operational processes can employ a more comprehensive set of privacy use cases to create architectures that build in privacy protections to mitigate identified privacy risks.
8. **Conclusions and recommendations**. This section summarizes the main points and findings on the subject of privacy and collects in one place all of the recommendations found within this Privacy Chapter.
9. **Appendices**. Reference material.

5.2 WHAT IS PRIVACY?

There is no one universal, internationally accepted definition of "privacy," it can mean many things to different individuals. At its most basic, privacy can be seen as the right to be left alone.[4] Privacy is not a plainly delineated concept and is not simply the specifications provided within laws and regulations. Furthermore, privacy should not be confused, as it often is, with being the same as confidentiality; and personal information[5] is not the same as confidential information. Confidential information[6] is information for which access should be limited to only those with a business need to know and that could result in compromise to a system, data, application, or other business function if inappropriately shared.[7]

It is important to understand that privacy considerations with respect to the Smart Grid include examining the rights, values, and interests of *individuals*; it involves the related characteristics, descriptive information and labels, activities, and opinions of individuals, to name just a few applicable considerations.

For example, some have described privacy as consisting of four dimensions:[8]

---

[4] Warren, Samuel D. and Louis D. Brandeis "The Right to Privacy," Harvard Law Review, Vol. IV December 15, 1890 No. 5

[5] See a full definition and discussion of "personal information" in Appendix C.

[6] The use of the phrase "confidential information" in this document does not refer to National Security/classified information.

[7] For example, market data that does not include customer-specific details is considered confidential. Other chapters within this report address confidentiality in depth.

[8] *See* Roger Clarke, "What's Privacy?" at http://www.rogerclarke.com/DV/Privacy.html. Clarke makes a similar set of distinctions between the privacy of the physical person, the privacy of personal behavior, the privacy of personal

1. **Privacy of personal information**. This is the most commonly thought-of dimension. Personal information is any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, locational or social identity. Privacy of personal information involves the right to control when, where, how, to whom, and to what extent an individual shares their own personal information, as well as the right to access personal information given to others, to correct it, and to ensure it is safeguarded and disposed of appropriately.
2. **Privacy of the person**. This is the right to control the integrity of one's own body. It covers such things as physical requirements, health problems, and required medical devices.
3. **Privacy of personal behavior**. This is the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others.
4. **Privacy of personal communications**. This is the right to communicate without undue surveillance, monitoring, or censorship.

Most Smart Grid entities directly address the first dimension, because most data protection laws and regulations cover privacy of personal information. However, the other three dimensions are important privacy considerations as well; thus dimensions 2, 3, and 4 should also be considered in the Smart Grid context because new types of energy use data can be created and communicated. For instance, we can recognize unique electric signatures for consumer electronics and appliances and develop detailed, time-stamped activity reports within personal dwellings. Charging station information can detail whereabouts of an EV. This data did not exist before the application of Smart Grid technologies.[9]

The privacy subgroup looked at how the Smart Grid, and the data contained therein, could potentially be used to infringe upon or otherwise negatively impact individuals' privacy in the four identified dimensions and then sought ways to assist Smart Grid organizations in identifying and protecting the associated information. While many of the types of data items accessible through the Smart Grid are not new, there is now the possibility that other parties, entities or individuals will have access to those data items; and there are now many new uses for the collected data, which may raise substantial privacy concerns. New energy use data is also created through applications of Smart Grid technologies. As those data items become more specific and are made available to additional individuals, the complexity of the associated privacy issues increases as well.

The mission of the privacy subgroup is to recognize privacy concerns within the Smart Grid and to identify opportunities and recommendations for their mitigation. In addition, the group strives to clarify privacy expectations, practices, and rights with regard to the Smart Grid by—

---

communications, and the privacy of personal data. Roger Clarke is a well-known privacy expert from Australia who has been providing privacy research papers and guidance for the past couple of decades.

[9] For instance, consider the enhanced ability the Smart Grid will give to determining a person's behavior within a home through more granular energy usage data.

- Identifying potential privacy problems and encouraging the use of relevant Fair Information Practice Principles[10]
- Seeking input from representatives of Smart Grid entities and subject matter experts, and then providing guidance to the public on options for protecting the privacy of—and avoiding misuse of—personal information used within the Smart Grid. This guidance is included in this chapter; and
- Making suggestions and providing information to organizations, regulatory agencies, and Smart Grid entities in the process of developing privacy policies and practices that promote and protect the interest of Smart Grid consumers and Smart Grid entities.

To meet this mission, this chapter explores the types of data within the Smart Grid that may place individuals' privacy at risk, and how the privacy risks related to the use, misuse, and abuse of energy data may increase as a result of this new, always-connected type of technology network.

Because "privacy" and associated terms mean many different things to different audiences, definitions for the privacy terms used within this chapter are found in Appendix C, and definitions for energy terms are included in Appendix I.

5.3 LEGAL FRAMEWORKS AND CONSIDERATIONS

5.3.1 Overview

In assessing privacy considerations and related legal impacts within the Smart Grid, it is important to understand existing regulatory and legislative frameworks, concepts, and definitions. This subsection discusses these themes in general terms and then narrows its focus to those deemed most relevant.

5.3.2 Existing Regulatory Frameworks

When considering the possible legal impacts to privacy engendered by the Smart Grid, and likewise the influence of laws that directly apply to the Smart Grid, it is important to note that current privacy laws may not explicitly reference the Smart Grid or associated unique Smart Grid data items. Moreover, existing U.S. state-level Smart Grid and electricity delivery regulations may not explicitly reference privacy protections.[11] However, even though Federal or State laws may not definitively reference the Smart Grid at this time, it is possible that existing laws may be amended to explicitly apply to the Smart Grid as as it is more widely implemented and touches more individuals.

While it is uncertain how privacy laws will apply to Smart Grid data, one thing that is certain is that the Smart Grid brings new challenges and issues with its new types of data, such as detailed personal use patterns of all electrical appliances used by any individual within a premise, usage

[10] Fair Information Practice Principles describe the manner in which entities using automated data systems and networks should collect, use, and safeguard personal information to assure their practice is fair and provides adequate information privacy protection.

[11] The SGIP-CSWG Privacy Group has compiled a list of most state Smart Grid and electricity delivery regulations and provided them in Appendix A as a useful resource for our readers.

patterns of all electrical appliances used in public, commercial and educational facilities, and fingerprint information about new device usage, including medical devices and vehicle charging data. These new data items, and the use of existing data in new ways, will require additional study and public input to adapt current laws or to shape new laws.

To understand the types of data items that may be protected within the Smart Grid by privacy laws and regulations, let us first consider some of the current and most prominent laws that provide for privacy protection. U.S. federal privacy laws cover a wide range of industries and topics, such as:

1. Healthcare: Examples include the Health Insurance Portability and Accountability Act (HIPAA) and the associated Health Information Technology for Economic and Clinical Health (HITECH) Act.
2. Financial: Examples include the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transactions Act (FACTA), and the Red Flags Rule.
3. Education: Examples include the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA).
4. Communications: Examples include the First Amendment to the U.S. Constitution, the Electronic Communications Privacy Act (ECPA), and the Telephone Consumer Protection Act (TCPA).
5. Government: Examples include the Privacy Act of 1974, the Computer Security Act of 1987, and the E-Government Act of 2002.
6. Online Activities: Examples include the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act, commonly known as the "Patriot Act").[12]
7. Privacy in the Home: Examples are the protections provided by the Fourth and Fourteenth Amendments to the U.S. Constitution.
8. Employee and Labor Laws: Examples include the Americans with Disabilities Act (ADA) and the Equal Employment Opportunity (EEO) Act.

It is currently not clear to what extent the above laws providing privacy protections will apply to Smart Grid data. Most state provides additional privacy laws and regulations for a wide range of issues, such as for, but not limited to, the following, which may also apply to the Smart Grid:

- Privacy breach notice;
- Social Security number (SSN) use and protections ; and
- Drivers license use.

There are generally three approaches to protecting privacy by law—

[12] The acronym stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. The statute enacted by the United States Government was signed into law on October 26, 2001.

- **Constitutional protections**. The First, Fourth, and Fourteenth Amendments, covering personal communications and activities.
- **Data-specific protections**. These protect specific information items such as credit card numbers and SSNs, or specific technology such as phones or computers used for data storage or communication.
- **Contractual protections**. These are protections specifically outlined within a wide range of business contracts, such as those between consumers and business.

The application of Fourth Amendment considerations to data collected about appliances and patterns of energy consumption, including the extent that Smart Grid data reveals information about personal activities, such as those described in "Privacy Concerns in the Smart Grid" (subsection 5.6 of this chapter) has not yet been tested.

Even though public utilities commissions (PUCs) have protected energy data in some states such as California, the energy-related data produced by the Smart Grid may not be covered by privacy protection laws that name specific data items. Energy consumption patterns have historically not risen to the level of public concern given to financial or health data because (1) electrical meters had to be physically accessed to obtain usage data directly from buildings, (2) the data showed energy usage over a longer time span such as a month and did not show usage by specific appliance, and (3) the utilities were not sharing this data in the ways that will now be possible with the Smart Grid. Public concerns for the related privacy impacts will likely change with implementation of the Smart Grid, because energy consumption data can reveal personal activities and the use of specific energy using or generating appliances, and because the data may be used or shared in ways that will impact privacy.

While some states have examined the privacy implications of the Smart Grid, most states had little or no documentation available for review by the privacy subgroup. Furthermore, enforcement of state privacy-related laws is often delegated to agencies other than PUCs, who have regulatory responsibility for electric utilities.

5.3.3 Smart Grid Data Ownership

The legal ownership of Smart Grid energy data is the subject of much discussion. Various regulators and jurisdictions have treated the issue of who owns energy data differently. However, regardless of data ownership, the management of energy data that contains or is combined with personal information or otherwise identifies individuals, and the personal information derived from such data, remains subject to the privacy considerations described in this report. The custodian of energy data should consider managing and safeguarding the information in accordance with the recommendations included in this report.

5.3.4 Applicability of Existing Data Protection Laws and Regulations to the Smart Grid

Personally identifiable information (PII) has no single authoritative legal definition. However, as noted in Appendix A, there are a number of laws and regulations, each of which protects different specific types of information. A number of these were previously noted, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which defines individually identifiable health information, arguably the widest definition by many organizations throughout the U.S. of what constitutes PII within the existing U.S. federal regulations. State attorneys general have pointed to HIPAA as providing a standard for defining

personal information, and to cite one case, the State of Texas has adopted the HIPAA requirements for protected health information to be applicable to all types of organizations, including all those based outside of Texas. Many of these organizations could possibly be providing information via the Smart Grid—if not now, then almost certainly at sometime in the future.[13]

The private industry's definition of personal information predates legislation and is generally legally defined in a two-step manner, as *x* data (e.g., SSN) in conjunction with *y* data (e.g., name.) This is the legal concept of "personally identifiable information" or PII.

For example, the Massachusetts breach notice law,[14] in line with some other state breach notice laws, defines the following data items as being personal information:

> First name and last name or first initial and last name in combination with any one or more of the following:
>
> 1. Social Security number;
> 2. Driver's license number or state-issued identification card number; or
> 3. Financial account number.

Utilities often store SSNs and financial account numbers in their payroll or billing systems and have been obligated to follow the associated legal requirements for safeguarding this data for many years. The sharing and storage capabilities that the Smart Grid network brings to bear creates the new need to protect the items specifically named within existing laws, in addition to protecting new types of personal information that is created within the Smart Grid.

There is also the possibility of utilities possessing new types of data as a result of the Smart Grid for which they have not to date been custodians. These new types of data may be protected by regulations from other industries that utilities did not previously have to follow. As is revealed by the privacy impact assessment that is the subject of section 5.4 of this chapter, there is a lack of privacy laws or policies directly applicable to the Smart Grid. Privacy subgroup research indicates that, in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid.[15] 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.[16]

---

[13] For example, the Texas Appellate Court stated that the HIPAA Privacy rule applies to the entire State of Texas. *See* Abbott v. Texas Department of Mental Health and Mental Retardation for details, or refer to the discussion at http://www.hipaasolutions.org/white_papers/HIPAA%20Solutions,%20LC%20White%20Paper%20-Texas%20AG%20Opinion%20On%20Privacy%20And%20HIPAA.pdf.

[14] *See* text of the Massachusetts breach notice law at http://www.mass.gov/legis/laws/seslaw07/sl070082.htm.

[15] Most public utility commissions have significant customer privacy policies that predate the Smart Grid.

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

The privacy subgroup is presently conducting an overview of the laws, regulations, and standards relevant to the privacy of energy consumption data, and its preliminary list of applicable state laws and regulations is given in Appendix A.

5.3.5 General Invasion of Privacy Concerns with Smart Grid Data

Two aspects of the Smart Grid may raise new legal privacy issues. First, the Smart Grid significantly expands the amount of data available in more granular form as related to the nature and frequency of energy consumption and creation, thereby opening up more opportunities for general invasion of privacy. Suddenly a much more detailed picture can be obtained about activities within a given dwelling, building, or other property, and the time patterns associated with those activities make it possible to detect the presence of specific types of energy consumption or generation equipment. Granular energy data may even indicate the number of individuals in a dwelling unit, which could also reveal when the dwelling is empty or is occupied by more people than usual. The public sharing of information about a specific location's energy use is also a distinct possibility. For example, a homeowner rigged his washing machine to announce the completion of its cycle via his social networking page so that the machine need not be monitored directly.[17] This raises the concern that persons other than those living within the dwelling but having access to energy data could likewise automate public sharing of private events without the dwellers' consent—a general invasion of privacy.

The concern exists that the prevalence of granular energy data could lead to actions on the part of law enforcement —possibly unlawful in themselves—and lead to an invasion of privacy, such as remote surveillance or inference of individual behavior within dwellings, that could be potentially harmful to the dwelling's residents. Law enforcement agencies have already used monthly electricity consumption data in criminal investigations. For example, in *Kyllo v. United States*,[18] the government relied on monthly electrical utility records to develop its case against a suspected marijuana grower.[19] Government agents issued a subpoena to the suspect's utility to obtain energy usage records and then used a utility-prepared "guide for estimating appropriate power usage relative to square footage, type of heating and accessories, and the number of people who occupy the residence" to show that the suspect's power usage was "excessive" and thus "consistent with" a marijuana-growing operation.[20]

As Smart Grid technologies collect more detailed data about households, one concern identified by the privacy group as well as expressed by multiple published comments is that law enforcement officials may become more interested in accessing that data for investigations or to develop cases. For instance, agencies may want to establish or confirm presence at an address at

[17] For a demonstration of how this was done, *see* the video, "Washing Machine Twitter Hack," by Ryan Rose at http://vimeo.com/2945872.

[18] *Kyllo v. United States*, 533 U.S. 27 (2001). *See* http://www.law.cornell.edu/supct/html/99-8508.ZO.html.

[19] *Id*. at page 30. The Supreme Court opinion in this case focuses on government agents' use of thermal imaging technology. However, the district court decision discusses other facts in the case, including that government agents issued a subpoena to the utility for the suspect's monthly power usage records. *See Kyllo v. United States*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd*, 190 F.3d 1041 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).

[20] *Kyllo v. United States*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd*, 190 F.3d 1041 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).

a certain critical time or even establish certain activities within the home —information that may be readily gleaned from Smart Grid data.

However, the Supreme Court in *Kyllo* clearly reaffirmed the heightened Fourth Amendment privacy interest in the home and noted this interest is not outweighed by technology that allows government agents to "see" into the suspect's home without actually entering the premises.[21] The Court stated, "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search" and is "presumptively unreasonable without a warrant."[22]

Second, unlike the traditional energy grid, the Smart Grid may be viewed as carrying private and/or confidential electronic communications between utilities and end-users, possibly between utilities and third parties[23], and between end-users and third parties. Current law both protects private electronic communications and permits government access to real-time and stored communications, as well as communications transactional records, using a variety of legal processes.[24] Moreover, under the Communications Assistance for Law Enforcement Act (CALEA), telecommunications carriers and equipment manufacturers are required to design their systems to enable lawful access to communications.[25] The granular Smart Grid data may also have parallels to call detail records collected by telecommunications providers. It is unclear if laws that regulate government access to communications will also apply to the Smart Grid.

In short, the innovative technologies of the Smart Grid pose new legal issues for privacy of the home, as well as any type of property location that has traditionally received strong Fourth Amendment protection. As Justice Scalia wrote in *Kyllo*: "The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[26]

5.3.6 Smart Grid Introduces a New Privacy Dimension

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 articles in the public media have raised serious concerns[27] about the type and amount of billing, usage, appliance, and other related information flowing throughout the various components of the Smart Grid.

---

[21] *Kyllo*, 533 U.S.

[22] *Kyllo*, 533 U.S.

[23] The term "third party" is one that is not well defined. The SGIP-CSWG privacy subgroup recognizes third party access as a significant issue and plans to address this in more depth in a future version of the chapter.

[24] Such as the Electronic Communications Privacy Act; 18 U.S.C. § 2510. *See* http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html.

[25] *See* http://thomas.loc.gov/cgi-bin/bdquery/z?d103:H.R.4922:.

[26] *Kyllo*, 533 U.S.

[27] One example of this is available at http://www.istockanalyst.com/article/viewiStockNews/articleid/3461363.

There are also concerns across multiple industries about data aggregation of "anonymized" data.[28] For example, in other situations, associating pieces of anonymized data with other publicly available non-anonymous data sets has been shown by various studies to actually reveal specific individuals.[29] Figure 5-1 illustrates how frequent meter readings may provide a detailed timeline of activities occurring inside a metered location and could also lead to knowledge about specific equipment usage or other internal home/business processes.

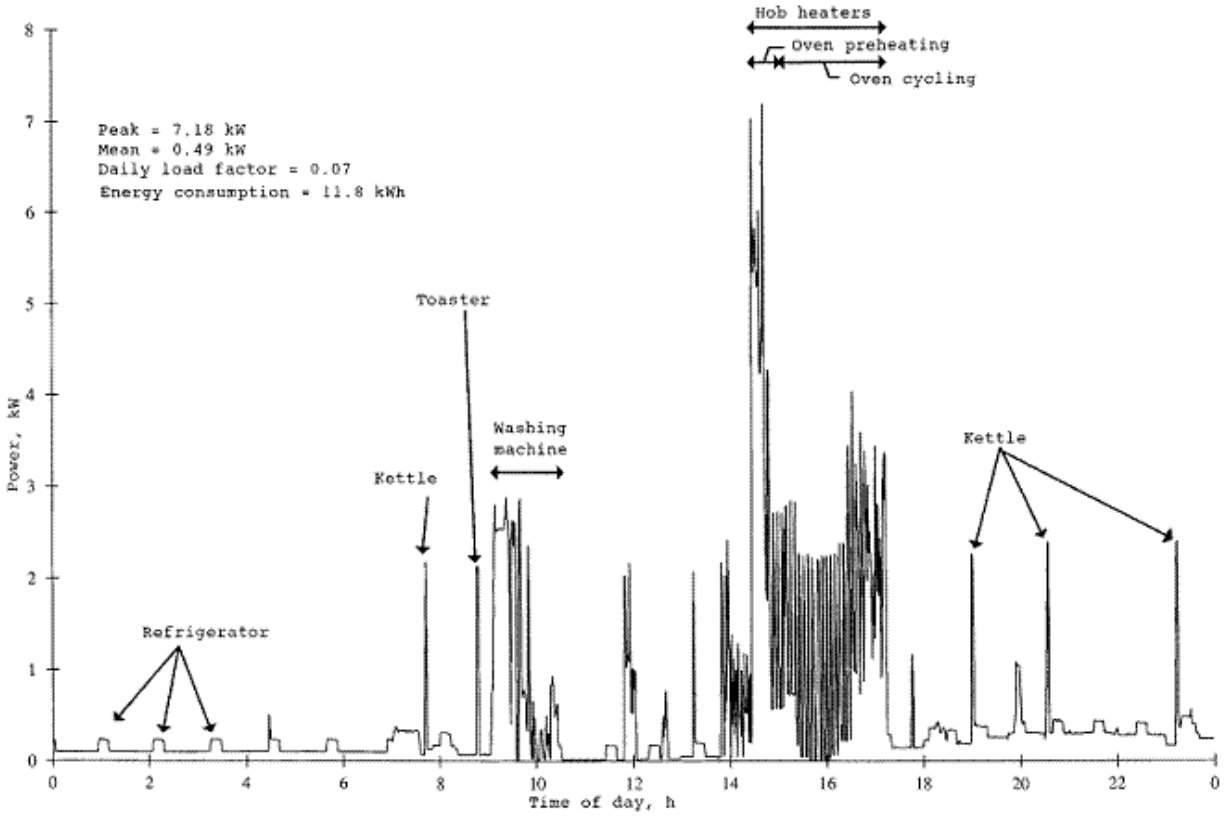

Figure 5-1 Power Usage to Personal Activity Mapping [30]

Smart meter data raises potential surveillance possibilities posing physical, financial, and reputational risks. Because smart meters collect energy usage data at much shorter time intervals than in the past (in 15-minute or sub-15-minute intervals rather than once a month), the information they collect can reveal much more detailed information about the activities within a dwelling or other premises than was available in the past. This is because smart meter data provides information about the usage patterns for individual appliances—which in turn can

28 The Electronic Privacy Information Center (EPIC), http://epic.org/privacy/reidentification/, provides news and resources on this topic.

[29] For one such 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.

[30] Elias Leake Quinn, *Smart Metering & Privacy: Existing Law and Competing Policies, Spring 2009*, at page 3. Available at http://www.dora.state.co.us/puc/DocketsDecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-Smart GridPrivacy.pdf. A hob heater is a top of stove cooking surface.

reveal detailed information about activities within a premise through the use of nonintrusive appliance load monitoring (NALM) techniques.[31] Using NALM, appliances' energy usage profiles can be compared to libraries of known patterns and matched to identify individual appliances.[32] For example, research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances.[33, 34] The graph shown above (Figure 5-1) depicts NALM results as applied to a household's energy use over a 24-hour period. NALM techniques have many beneficial uses, including pinpointing loads for purposes of load balancing or increasing energy efficiency. However, such detailed information about appliance use can also reveal whether a building is occupied or vacant, show residency patterns over time, and reflect intimate details of people's lives and their habits and preferences inside their homes.[35] In 1989, George W. Hart, one of the inventors of NALM, explained the surveillance potential of the technique in an article in IEEE Technology and Society Magazine.[36] As the time intervals between smart meter data collection points decreases, appliance use will be inferable from overall utility usage data and other Smart Grid data with even greater accuracy.

In general, 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. Figure 5-2 presents the NIST conceptual model illustrating how data collection can be expected to proliferate as networked grid components increase. 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). Further, once uniquely identifiable "smart" appliances are in use, they will communicate even more specific information directly to utilities, consumers, and other entities, thus adding to the detailed picture of activity within a premise that NALM can provide.

---

[31] *Id*. at page A-2. The development of NALM involved a real-time monitoring device attached to a meter to log energy consumption. Researchers then worked backward from that information using complex algorithms to reconstruct the presence of appliances. Since smart meters and these NALM devices operate similarly, the same research and techniques can be reused to identify appliances.

[32] *Id*. at page A-4 n.129 (discussing the maintaining of appliance profile libraries).

[33] Research suggests this can be done with accuracy rates of over 90 percent. *See* Elias Leake Quinn, *Privacy and the New Energy Infrastructure*, Feb. 15, 2009, http://ssrn.com/abstract=1370731, at page 28.

[34] *See also* Steven Drenker & Ab Kader, *Nonintrusive Monitoring of Electric Loads*, IEEE Computer Applications in Power at pages 47, 50 (1999), noting the near perfect identification success rate in larger two-state household appliances such as dryers, refrigerators, air conditioners, water heaters, and well pumps. *Available at* http://ieeexplore.ieee.org/iel5/67/17240/00795138.pdf?arnumber=795138.

[35] For instance, daily routines such as showers and baths could be identified, as well as whether the customer "prefers microwave dinners to a three-pot meal." *Id*. Quinn, *Privacy and the New Energy Infrastructure*, at page 5.

[36] George W. Hart, Residential Energy Monitoring and Computerized Surveillance via Utility Power Flows, IEEE Technology and Society Magazine, June 12, 1989, http://ieeexplore.ieee.org/iel5/44/1367/00031557.pdf?arnumber=31557.

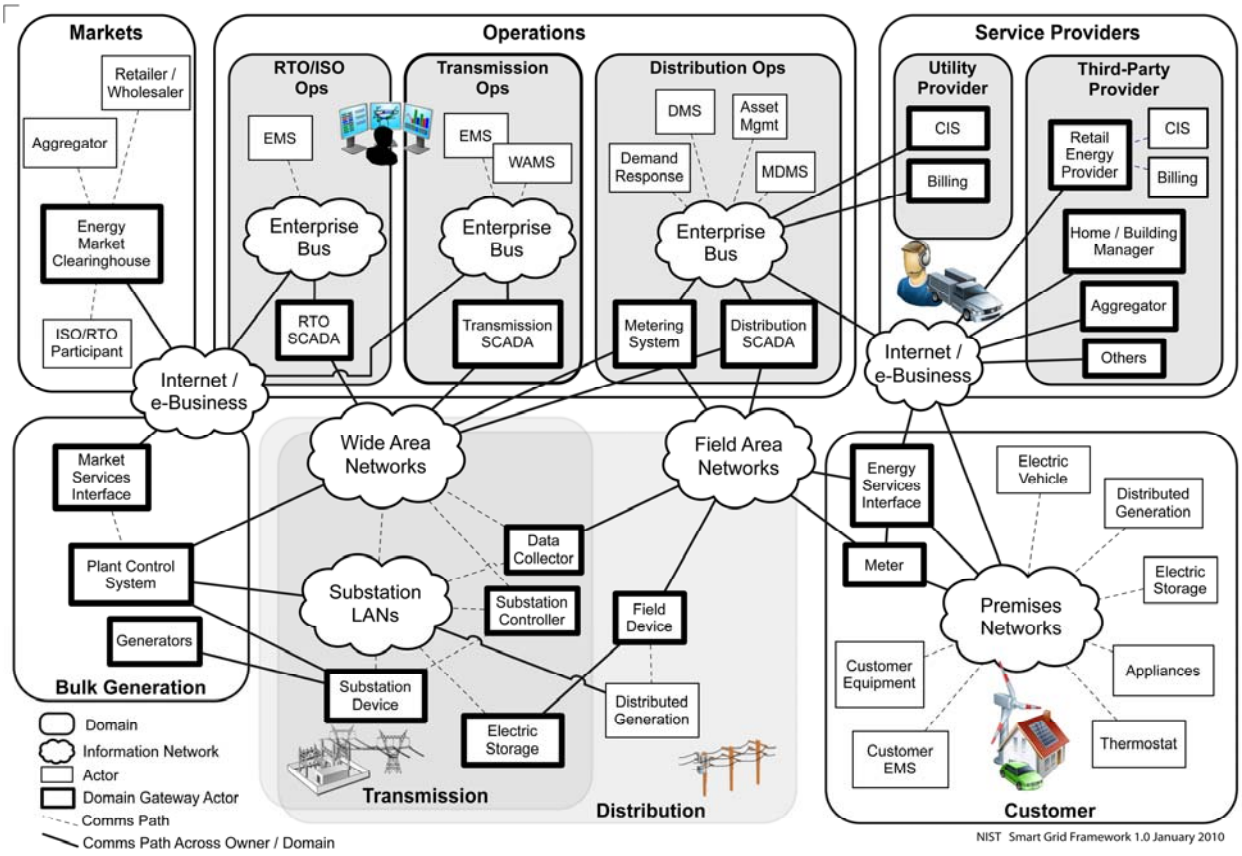

Figure 5-2 NIST Conceptual Model [37]

The proliferation of smart appliances, utility devices, and devices from other entities throughout the Smart 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 consumer side of the meter are expanded when these appliances and devices transmit data outside of the home area network (HAN) or energy management system (EMS) 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 plug-in electric vehicles (PEVs). Charging data may be used to track the travel times and locations for the PEV owners.

5.4 CONSUMER-TO-UTILITY PRIVACY IMPACT ASSESSMENT

A PIA is a comprehensive process for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information. PIAs also define the measures that may be used to mitigate and, wherever possible, eliminate the identified risks. The Smart Grid PIA activity provides a structured, repeatable type of analysis aimed at determining how collected data can reveal personal information about individuals or groups of individuals, and the focus of the PIA can be on a segment within the grid or the grid as a whole. Privacy risks

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

may be addressed and mitigated by policies and practices that are instituted throughout the implementation, evolution, and ongoing management of the Smart Grid.

The privacy subgroup conducted a PIA for the consumer-to-utility portion of the Smart Grid during August and September 2009. In the months following the PIA, the group considered additional privacy impacts and risks throughout the entire Smart Grid structure.

The focus of the privacy subgroup has been on determining (1) the types of information that may be collected or created that can then reveal information about individuals or activities within specific premises (both residential and commercial), (2) determining how these different types of information may be exploited, and (3) recommending business policies and practices to mitigate the identified privacy risks. Entities of all types that provide, use, or obtain data from the Smart Grid can also benefit from performing PIAs to determine privacy risks and then take action to mitigate those risks.

The following questions were identified and addressed in the process of performing the consumer-to-utility PIA and in the follow-on discussion of the findings:

1. What personal information may be generated, stored, transmitted, or maintained by components and entities of the Smart Grid?
2. How is this personal information new or unique compared with personal information in other types of systems and networks?
3. How is the use of personal information within the Smart Grid new or different from the uses of the information in other types of systems and networks?
4. What are the new and unique types of privacy risks that may be created by Smart Grid components and entities?
5. What is the potential that existing laws, regulations, and standards apply to the personal information collected by, created within, and flowing through the Smart Grid components?
6. What could suggested standardized privacy practices look like for all entities using the Smart Grid so that following them could help to protect privacy and reduce associated risks?

5.4.1 Consumer-to-Utility PIA Basis and Methodology

In developing a basis for the consumer-to-utility PIA, the privacy subgroup reviewed the available documentation for use cases for the Advanced Metering Infrastructure (AMI)[38] and other published Smart Grid plans covering the interactions between the consumers of services and the providers of those services. The group also reviewed numerous data protection requirements and considered global information security and privacy protection laws, regulations, and standards to assemble the criteria against which to evaluate the consumer-to-utility aspects of Smart Grid operations. Taken into account were numerous U.S. federal data protection requirements and Fair Information Practice Principles, also often called "Privacy Principles," that are the framework for most modern privacy laws around the world. Several

[38] *See* "AMI Systems Use Cases" at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/AugustWorkshop/All_of_the_Diagrams_in_one_document.pdf.

versions of the Fair Information Practice Principles have been developed through government studies, federal agencies, and international organizations.

For the purposes of this PIA, the group used the American Institute of Certified Public Accounts (AICPA) Generally Accepted Privacy Principles (GAPPs),[39] the Organisation for Economic Cooperation and Development (OECD) Privacy Principles, and information security management principles from the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) *International Standard ISO/IEC 27001*[40] as its primary evaluation criteria:

- The ten AICPA principles are entitled Management, Notice, Choice and Consent, Collection, Use and Retention, Access, Disclosure to Third Parties, Security for Privacy, Quality, and Monitoring and Enforcement.
- With respect to the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,*[41] the group's particular focus was on the *Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,*[42] wherein paragraphs 7–14 of Part Two[43] outline the basic principles of national application, and on the "Explanatory Memorandum,"[44] wherein those principles are amplified (by paragraph number) in subsection II.B.[45] The enumerated OECD principles relate to Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Openness, and Individual Participation.
- *International Standard ISO/IEC 27001* provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS).

The general privacy principles and ISMS described here and adopted for use in the PIA are designed to be applicable across a broad range of industries and are considered internationally to be best practices but are generally not mandatory. However, most privacy experts agree that data protection laws throughout the world have been built around these principles.

5.4.2 Summary PIA Findings and Recommendations

The consumer-to-utility PIA conducted by the privacy subgroup revealed valuable insights about the general consumer-to-utility data flow and privacy concerns, and indicated that significant areas of concern remain to be addressed within each localized domain of the Smart Grid. For

[39] *See* "AICPA's Generally Accepted Privacy Principles" at http://www.compliancebuilding.com/2009/01/09/aicpas-generally-accepted-privacy-principles/.

[40] *See* http://webstore.iec.ch/preview/info_isoiec27001%7Bed1.0%7Den.pdf.

[41] *See* full OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" at http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html.

[42] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#guidelines.

[43] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2.

[44] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#memorandum.

[45] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#comments.

example, as Smart Grid implementations collect more granular, detailed, and potentially personal information, this information may reveal business activities, manufacturing procedures, and personal activities in a given location. It will therefore be important for utilities to consider establishing privacy practices to protect this information.

As noted in section 5.3,[46] which focuses on privacy laws and legal considerations, the PIA also revealed the lack of privacy laws or policies directly applicable to the Smart Grid. Accordingly, opportunities remain for developing processes and practices to identify and address Smart Grid privacy risks.

Organizations that collect or use Smart Grid data can use the Privacy Group's PIA findings to guide their own use of PIAs and develop appropriate systems and processes for Smart Grid data. Organizations can also use the six questions listed in subsection 3.5 (p. 16) when conducting their own PIAs and then examine their findings with the ten privacy principles listed below. The answers to these questions are essential both for efficient data management in general and for developing an approach that will address privacy impacts in alignment with all other organizational policies regarding consumer data. Where an organization has defined privacy responsibilities, policies, and procedures, that organization should consider reviewing its responsibilities and updating or potentially augmenting its policies and procedures to address the new privacy issues associated with the Smart Grid. Each entity within the Smart Grid can follow a similar methodology to perform its own PIAs to ensure privacy is appropriately addressed for its Smart Grid activities.

The following points summarize the PIA findings and recommendations as presented in the draft *NIST Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment*[47] in relation to the privacy principles used as the basis for the PIA. Each enumerated privacy principle statement is followed by the related findings from the PIA and the suggested privacy practices that may serve to mitigate the privacy risks associated with each principle:

1. **Management and Accountability**: Organizations that access or provide data to the Smart Grid should appoint personnel to a position responsible for ensuring that documented information security and privacy policies and practices exist and are followed. Information security and personal information privacy practices should include requirements for regular training and ongoing awareness activities. Audit functions should also be present to monitor the Smart Grid data access activities.

   Findings:

   Some organizations that participate within the Smart Grid (1) do not have documented information security and privacy responsibilities and authority within the organization; (2) do not have information security and privacy training and awareness programs; and (3) do not monitor access to Smart Grid data.

[46] *See* 5.3.2, Existing Regulatory Frameworks, and 5.3.4, Applicability of Existing Data Protection Laws and Regulations to the Smart Grid.

[47] *See* full draft PIA report at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/NIST_High_Level_PIA_Report_-_Herold_09_09_09_w-edits.doc.

Privacy Practices Recommendations:

- **Assign privacy responsibility**. Each organization collecting or using Smart Grid data from or about consumer locations should create (or augment) a position or person with responsibility to ensure that privacy policies and practices exist and are followed. Responsibilities should include documenting, ensuring the implementation of, and managing requirements for regular training and ongoing awareness activities.
- **Establish privacy audits**. Audit functions should be modified to monitor all energy data access.
- **Establish law enforcement request policies and procedures**. Organizations accessing, storing, or processing energy data should include specific documented incident response procedures for incidents involving energy data.

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

   Findings:

   The data obtained from systems and devices that are part of the Smart Grid 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.

   Privacy Practices Recommendations:

   - **Provide notification for the personal information collected**. Any organization collecting energy data from or about consumers should establish a process to notify consumer account 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 the intended use, retention, and sharing of the data. This notification should include information about when and how information may or may not be shared with law enforcement officials. Individuals should be notified before the time of collection.
   - **Provide notification for new information use purposes and collection**. Organizations should update consumer notifications whenever they want to start using existing collected data for materially different purposes other than those the consumer has previously authorized. Also, organizations should notify the recipients of services whenever they want 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 consumers with regard to the use of their associated energy data that could be used to reveal personal information and obtain explicit consent, if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of this information.

Findings:

Currently it is not 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 and other smart devices increase capabilities and expand sharing of the data throughout the Smart Grid, organizations should establish processes to give consumers a choice, where possible and feasible, about the types of data collected and how it is used.

Privacy Practices Recommendation:

- **Provide notification about choices**. The consumer 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) explaining when and why data items are or may be collected and used without obtaining consent, such as when certain pieces of information are needed 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 consumers. This information should be obtained by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.

   Findings:

   In the current operation of the electric utilities, data taken from traditional meters consists of basic data usage readings required to create bills. Under the Smart Grid implementation, smart meters will be able to collect other types of data. Home power generation services will also likely increase the amount of information created and shared. Some of this additional data may constitute personal information or may be used to determine personal activities. Because of the associated privacy risks, only the minimum amount of data necessary for services, provisioning, and billing should be collected.

   Privacy Practices Recommendations:

   - **Limit the collection** of data to only that necessary for Smart Grid operations, including planning and management, improving energy use and efficiency, account management, and billing.
   - **Obtain the data** by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.

5. **Use and Retention**: Information within the Smart Grid should be used or disclosed only for the purposes for which it was collected. Smart Grid data should be aggregated in such a way that personal information or activities cannot be determined, or anonymized wherever possible to limit the potential for computer matching of records. Personal information should be kept only as long as is necessary to fulfill the purposes for which it was collected.

Findings:

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

Privacy Practices Recommendations:

- **Review privacy policies and procedures**. Every organization with access to Smart Grid data should review existing information security and privacy policies to determine how they may need to be modified. This review should include privacy policies already in place in other industries, such as financial and healthcare, which could provide a model for the Smart Grid.
- **Limit information retention**. Data, and subsequently created information that reveals personal information or activities from and about a specific consumer location, should be retained only for as long as necessary to fulfill the purposes that have been communicated to the energy consumers. 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 data becomes more granular, more refined, and has more potential for commercial uses.

6. **Individual Access**: Organizations should provide a process to allow for individuals to request access to see their corresponding personal information and energy data, and to request the correction of real or perceived inaccuracies. Personal information individuals should also be informed about parties with whom their associated personal information and energy data has been shared.

   Findings:

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

   Privacy Practices Recommendations:

   - **Consumer access**. Any organization possessing energy data about consumers should provide a process to allow consumers access to the corresponding energy data for their utilities account.
   - **Dispute resolution**. Smart Grid entities should establish documented dispute resolution procedures for energy consumers to follow.

7. **Disclosure and Limiting Use**: Personal information should not be disclosed to any other parties except those identified in the notice and only for the purposes originally specified or with the explicit informed consent of the service recipient.

   Findings:

   As Smart Grid implementations collect more granular and detailed information, this information is capable of revealing 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 individuals or organizations to which the information applies.

Privacy Practices Recommendation:

- **Limit information use**. Data on energy or other Smart Grid service activities should be used or disclosed only for the authorized purposes for which it was collected.
- **Disclosure**. Data should be divulged to or shared only with those parties authorized to receive it and with whom the organizations have told the recipients of services it would be shared.

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

   Findings:

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

   Privacy Practices Recommendations:

   - **Associate energy data with individuals only when and where required**. For example only link equipment data with a location or consumer 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 all entities obtaining or using this data as the Smart Grid is further deployed.
   - **De-identify information**. Energy 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 that energy data from specific consumer locations is limited appropriately. This may not be possible for some business activities, such as for billing.
   - **Safeguard personal information**. All organizations collecting, processing, or handling energy data and other personal information from or about consumer locations should ensure that all information collected and subsequently created about the recipients of Smart Grid services is appropriately protected in all forms from loss, theft, unauthorized access, disclosure, copying, use, or modification. While this practice is commonly in effect in the utility industry, as other entities recognize commercial uses for this information, they too should adopt appropriate requirements and controls. In addition, given the growing granularity of information from Smart Grid operations, the responsibility for these existing policies should be reviewed and updated as necessary.
   - **Do not use personal information for research purposes**. Any organization collecting energy data and other personal information from or about consumer

locations should refrain from using actual consumer data for research until it has been anonymized and/or sufficiently aggregated to assure to a reasonable degree the inability to link detailed data to individuals. Current and planned research is being conducted both inside and outside the utility industry on the Smart Grid, its effects upon demand response, and other topics. The use of actual information that can be linked to a consumer in this research increases the risk of inadvertent exposure via traditional information sharing that occurs within the research community.

9. **Accuracy and Quality**: Processes should be implemented by all businesses participating within the Smart Grid to ensure as much as possible that energy data and personal information are accurate, complete, and relevant for the purposes identified in the notice [*see* §5.4.2-2], and that it remains accurate throughout the life of the energy data and personal information while within the control of the organization.

   Findings:

   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 and the information's accuracy. Since Smart Grid data may be stored in many locations, and therefore be accessed by many different individuals/entities and used for a wide variety of purposes, personal information may be inappropriately modified. Automated decisions about energy use could be detrimental for consumers (e.g., restricted power, thermostats turned to dangerous levels, and so on) if it happens that decisions about energy usage are based upon inaccurate information.

   Privacy Practices Recommendation:

   - **Keep information accurate and complete**. Any organization collecting energy data from or about consumer locations should establish 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 identified purposes for which they were obtained, and that it 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 to review and a process by which to challenge an organization's compliance with the applicable privacy protection legal requirements, along with the associated organizational privacy policies and the organizations' actual privacy practices.[48]

    Findings:

    Currently electric utilities follow a wide variety of methods and policies for communicating to energy consumers how energy data and personal information is used. The data collected from smart meters and related Smart Grid equipment will potentially be stored in multiple locations throughout the Smart Grid, possibly within multiple states

[48] Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the Federal Trade Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information.

and outside the United States. This complicates the openness of organizational privacy compliance and of a consumer being able to challenge the organization's compliance with privacy policies, practices, and applicable legal requirements.

Privacy Practices Recommendations:

- **Policy challenge procedures**. Organizations collecting energy data, and all other entities throughout the Smart Grid, should establish procedures that allow Smart Grid consumers to have the opportunity and process to challenge the organization's compliance with their published privacy policies as well as their actual privacy practices.
- **Perform regular privacy impact assessments**. Any organization collecting energy data from or about consumer locations should perform periodic PIAs with the proper time frames, to be determined by the utility and the appropriate regulator, based upon the associated risks and any recent process changes and/or security incidents. The organizations should consider sending a copy of the PIA results for review by an impartial third party and making the results of the review public. This will help to promote compliance with the organization's privacy obligations and provide an accessible public record to demonstrate the organization's privacy compliance activities. Organizations should also perform a PIA on each new system, network, or Smart Grid application and consider providing a copy of the results in similar fashion to that mentioned above.
- **Establish breach notice practices**. Any organization with Smart Grid data should establish policies and procedures to identify breaches and misuse of Smart Grid data, along with expanding or establishing procedures and plans for notifying the affected individuals 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 service providers).

5.5 PERSONAL INFORMATION IN THE SMART GRID

As the PIA showed, energy data and personal information can reveal something either explicitly or implicitly about specific individuals, groups of individuals, or activities of those individuals. Smart Grid data such as energy usage measurements, combined with the increased frequency of usage reporting, energy generation data, and the use of appliances and devices capable of energy consumption reporting, provide new sources of personal information.

The personal information traditionally collected by utility companies can be used to identify individuals through such data as house number and/or street address, homeowner or resident's first, middle, or last name, date of birth, and last four digits of the SSN. Smart Grid data elements that reflect the timing and amount of energy used, when correlated with traditional personal information data elements, can provide insights into the life style of residential consumers and the business operations of commercial and industrial consumers.[49]

[49] The ability to determine personal activities according to energy consumption data alone was demonstrated recently in quotes from a Siemens representative in an article published in the Washington Post: "We, Siemens, have the technology to record it (energy consumption) every minute, second, microsecond, more or less live," said Martin

With a few exceptions (e.g., SSN and credit card numbers), rarely does a single piece of information or a single source permit the identification of an individual or group of individuals. However, in recent years it has been shown through multiple research studies[50] and incidents[51] that a piece of seemingly anonymous data (date of birth, gender, zip code) that on its own cannot uniquely identify an individual may reveal an individual when combined with other types of anonymous data. If different datasets that contain anonymized data have at least one type of information that is the same, the separate sets of anonymized information may have records that are easily matched and then linked to an individual. It is also possible the matches to an individual may be narrowed to the point that linking becomes an easy task.[52] (This may particularly be seen in sparsely populated geographical areas.)

Another study published in 2009 illustrates the increasing ease of aggregating data into personally identifiable information. Carnegie Mellon researchers Alessandro Acquisti and Ralph Gross assessed the predictability of SSNs by knowing the date and geographic location of an individual subject's birth and found that they could predict the first five digits for 44% of those born after 1988 on the first attempt and 61% within two attempts.[53]

Pollock of Siemens Energy, an arm of the German engineering giant, which provides metering services. "From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data." *See* "Privacy concerns challenge smart grid rollout," Reuters, June 25, 2010; http://www.reuters.com/article/idUSLDE65N2CI20100625.

[50] *See* Arvind Narayanan and Vitaly Shmatikov, Privacy and Security: Myths and Fallacies of "Personally Identifiable Information," Communications of the ACM, available at http://userweb.cs.utexas.edu/~shmat/shmat_cacm10.pdf. June 2010. This article points out multiple incidents and studies that have shown how combinations of data items that are anonymous individually can be linked to specific individuals when combined with other anonymous data items and "quasi-identifiers" or a piece of auxiliary information. "Consumption preferences" is specifically named as a type of human characteristic data that, when combined with other items, can point to individuals.

[51] In addition to the incidents discussed in the Narayanan and Shmatikov article previously referenced, another specific example to consider is that in 2006, AOL released anonymous information about search data that was re-identified linking to individuals by a NY Times reporter. This incident led to a complaint filed by the Electronic Frontier Foundation (EFF) with the Federal Trade Commission against AOL for violating the Federal Trade Commission Act. *See* Michael Barbaro & Tom Zeller, Jr., "A Face is Exposed for AOL Searcher No. 4417749," N.Y. TIMES, Aug. 9, 2006, at §A1, available at http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000.

[52] Latanya Sweeney, "k-anonymity: A Model for Protecting Privacy, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems," 10(5), 2002; pages 557-570, available at http://epic.org/privacy/reidentification/Sweeney_Article.pdf. Sweeney gathered data from the Massachusetts Group Insurance Commission (GIC), which purchases health insurance for state employees. GIC released insurer records to the researcher, but before doing so, with the support of the Governor's office, they removed names, addresses, SSNs, 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. Matched with the voter rolls, the GIC database showed 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. Correlating information in the voter rolls with the GIC database made it possible to re-identify the Governor's records in the GIC data, including his prescriptions and diagnoses.

[53] Alessandro Acquisti and Ralph Gross, Predicting Social Security numbers from public data, July 7, 2009, at http://www.pnas.org/content/106/27/10975.full.pdf+html.

These cases show that data can sometimes be re-identified to specific individuals by comparing anonymized information to generally available information, or by combining two datasets to produce new and more sensitive data which was not originally contained in either dataset.

There are potential unintended consequences of seemingly anonymous Smart Grid data being compiled, stored, and cross-linked. One concern is that combining Smart Grid data, which may be considered anonymous, with other types of anonymous information might lead to identifying individuals or groups of individuals associated with an address. Computing technology and the use of certain algorithms makes this type of process much easier.

While current privacy and security anonymization practices tend to focus on the removal of specific personal information data items, the studies referenced in this section show that re-identification[54] and linking to an individual may still occur. This issue of data re-identification becomes potentially more significant as the amount and granularity of the data being gathered during Smart Grid operations increases with the deployment of more Smart Grid components. It then becomes important, from a privacy standpoint, for utilities and third parties participating in the Smart Grid to determine which data items will remove the ability to link to specific addresses or individuals whenever they perform their data anonymization[55] activities.

Table 5-1 identifies and describes potential data elements within the Smart Grid that could impact privacy if not properly safeguarded.

Table 5-1 Information potentially available through the Smart Grid

Data Element(s)	Description
Name	Party responsible for the account
Address	Location where service is being taken
Account Number	Unique identifier for the account
Meter reading	kWh energy consumption recorded at 15–60 (or shorter) minute intervals during the current billing cycle
Current bill	Current amount due on the account
Billing history	Past meter reads and bills, including history of late payments/failure to pay, if any
Home area network	Networked in-home electrical appliances and devices
Lifestyle	When the home is occupied and unoccupied, when occupants are awake and asleep, how much various appliances are used
Distributed resources	The presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns
Meter IP	The Internet Protocol address for the meter, if applicable

[54] *Re-identification* is the process of relating unique and specific entities to seemingly anonymous data, resulting in the identification of individuals and/or groups of individuals.

[55] *Data Anonymization* is a process, manual or automated, that removes, or replaces with dummy data, information that could identify an individual or a group of individuals from a communication, data record, or database.

Service provider	Identity of the party supplying this account (relevant only in retail access markets)

5.6 IN-DEPTH LOOK AT SMART GRID PRIVACY CONCERNS

As outlined in the results of the PIA described earlier, there is a wide range of privacy concerns to address within the Smart Grid. These 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 consumer 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; and
- Type II: Mechanisms for obtaining (or manipulating) personal information that did not previously exist.

Examples of Type I concerns include detailed information on the appliances and equipment in use at a given location, including the use of specific medical devices and other electronic devices that indicate personal patterns and timings of legal and potentially illegal operations within the location, and finely grained time series data on power consumption at metered locations and from individual appliances.

Type II concerns include 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 PEVs raises the possibility of tracking physical location through new energy consumption data.

Detailed pictures of activities within a house or building can be derived from "equipment electricity signatures"[56] and their time patterns. Such signatures and patterns can provide a basis for making assumptions about occupant activities (e.g., the number of individuals at a location and when the premise 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 detailed energy consumption information to both their owners and operators—and to outside parties.

Table 5-2 outlines some of the possible areas of privacy concern and provides some analysis of the nature of the concern according to the Type I and II categories given above. While this is not an exhaustive list, it serves to help categorize the concerns noted.

[56] This is a term coined by our Privacy Group and not one that is officially used by any regulatory or standards group.

Table 5-2 Potential Privacy Concerns and Descriptions

Privacy Concern	Discussion	Categorization
Fraud	Attributing energy consumption to another location or vehicle (in the case of PEVs).	Type II: While fraud is an existing concern, the current system of reading consumer meters (either manual recording or electronically via "drive-by" remote meter reading systems) may allow less opportunity for data manipulation without collusion with the personnel collecting the data.
Determine Personal Behavior Patterns / Appliances Used	Smart meter and home automation network data may track the use of specific 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. Possible uses for this information include: Appliance manufacturers could use this information for product reliability and warranty purposes; Other entities could use this data to do targeted marketing.	Type I: The type of data made available by Smart Grid implementation may be both more granular and available on a broader scale.
Perform Real-Time Remote Surveillance	Access to live energy use data can reveal such things as if people are in a facility or residence, what they are doing, waking and sleeping patterns, where they are in the structure, and how many are in the structure.	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. Universities might purchase information to study student attributes and target a new student profile with simple application question profiling. Such profiling could extend to other types of profiling on employment selection, rental applications, and other situations that may not be welcomed by those targets.	Type II: 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 that 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.

5.6.1 Data Collection and Availability

A detailed sense of activities within a house or building can be derived from equipment electricity signatures, individual appliance usage data, time patterns of usage, and other data, as illustrated at the beginning of this chapter (subsection 5.3.6, Figure 5-1). Especially when collected and analyzed over a period of time, this information can provide a basis for potentially determining about occupant activities and lifestyle. For example, a forecast may be made about the number of individuals at a premise, when the location is unoccupied, sleep schedules, work schedules, and other personal routines.[57]

While technology that communicates directly with appliances and other energy consumption elements already exists, Smart Grid implementation may create broader incentives for its use and provide easier access by interested parties. Appliances so equipped may deliver granular energy consumption data to both their owners and operators, as well as to outside parties. The increased collection of and access to granular energy usage data will create new uses for that data: for example, residential demand-response systems,[58] marketing,[59] and law enforcement.[60] Many of these new uses will be innovative and provide individual and consumer benefits, some will impact privacy, and many will do both.

The listing of "Potential Privacy Concerns and Descriptions" shown earlier (Table 5-2), outlines some of the likely uses of Smart Grid data and maps them to privacy concerns that arise from new uses. The table also lists a variety of parties that are likely to use Smart Grid data. Many of these uses are legitimate and beneficial. However, all parties that collect and use Smart Grid data should be aware of uses that impact privacy and should develop appropriate plans for data stewardship, security, and data use. Any party could intentionally or unintentionally be the source of data that is misused or that is used in a way that has negative effects on consumer privacy. "Intentional" privacy compromises might occur through voluntary disclosure of data to third parties who then share the data with others or use the data in unexpected ways, while "unintentional" impacts might arise through data breaches or criminal attacks. It is important that all Smart Grid entities handling personal information to be aware of the various possible uses of

[57] *See* Mikhail Lisovich, Deirdre Mulligan, & Stephen Wicker, *Inferring Personal Information from Demand-Response Systems*, IEEE Security & Privacy, Jan.-Feb. 2010, at pages 11-20 (presenting the results of an initial study in the types of information than can be inferred from granular energy consumption data).

[58] Federal Energy Regulatory Commission, *Assessment of Demand Response & Advanced Metering 2008, Staff Report*, Dec. 2008, available at http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf (discussing various types of demand-response systems and pricing schemes, including those for residential *customers).*

[59] Martin LaMonica, *Microsoft Dials Hohm to Cut Home Energy Use*, CNET, June 23, 2009, *available at* http://news.cnet.com/8301-11128_3-10269832-54.html (describing Microsoft's business model for monetizing its energy consumption web application as selling contextual ads to generate revenue in the beginning, but eventually "Microsoft anticipates that it can become a sort of information broker between customers and utilities looking for ways to improve the efficiency of their customers").

[60] Law enforcement already uses energy consumption data to try to identify potentially criminal activity, like drug cultivation. *See e.g.*, Jo Moreland, *Drug Raid Has Carlsbad Family Seeing Red*, N. County Times, Mar. 25, 2004, available at http://www.nctimes.com/news/local/article_ea2047e8-59e1-551e-b173-ce89ffad4d90.html. More granular data will provide them with more valuable information that may be able to identify a wider range of illegal activities.

the data, and that they consider these factors when developing processes for data collection, handling, and disclosure.

Many potential uses arise from the generation of granular energy data, especially when it is combined with personal information. Table 5-3 broadly illustrates the various industries that may be interested in Smart Grid data. While this is not an exhaustive listing, it serves to help categorize the various concerns.

Table 5-3 Potential Privacy Impacts that Arise from the Collection and Use of Smart Grid Data

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
Captures detailed energy usage at a location, whether in real-time or on a delayed basis.	*Personal Behavior Patterns and Activities Inside the Home* Behavioral patterns, habits, and activities taking place inside the home by monitoring electricity usage patterns and appliance use, including activities like sleeping, eating, showering, and watching TV. Patterns over time to determine number of people in the household, work schedule, sleeping habits, vacation, health, affluence, or other lifestyle details and habits. When specific appliances are being used in a home, or when industrial equipment is in use, via granular energy data and appliance energy consumption profiles. *Real-Time Surveillance Information* Via real-time energy use data, determine if anyone is home, what they are doing, and where they are located in the home.	Utilities	Primary	Load monitoring and forecasting; demand response; efficiency analysis and monitoring, billing.
		Edge Services[62]		Efficiency analysis and monitoring; demand-response, public or limited disclosure to promote conservation, energy awareness, etc. (e.g., posting energy usage to social media).
		Insurance Companies	Secondary	Determine premiums (e.g., specific behavior patterns, like erratic sleep, that could indicate health problems).
		Marketers		Profile for targeted advertisements.
		Law Enforcement		Identify suspicious or illegal activity; investigations; real-time surveillance to determine if residents are present and current activities inside the home.
		Civil Litigation		Determine when someone was home or the number of people present.
		Landlord/Lessor		Use tenants' energy profiles to verify lease compliance.
		Private Investigators		Investigations; monitoring for specific events.
		The Press		Public interest in the activities of famous individuals.[63]

[61] "Primary" uses of Smart Grid data are those used to provide direct services to customers that are directly based on that data, including energy generation services or load monitoring services. "Secondary" uses of data are uses that apply Smart Grid data to other business purposes, such as insurance adjustment or marketing, or to nonbusiness purposes, such as government investigations or civil litigation. "Illicit" uses of data are uses that are never authorized and are often criminal.

[62] Edge services include businesses providing services based directly upon electrical usage but not providing services related to the actual generation, transportation, or distribution of electricity. Some examples of edge services would include Google PowerMeter, Microsoft Hohm, or consulting services based upon electricity usage.

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
		Creditors		Determine behavior that seems to indicate creditworthiness or changes in credit risk.[64]
		Criminals and Other Unauthorized Users	Illicit	Identify the best times for a burglary; determine if residents are present; identify assets that might be present; commit fraud; identity theft; disrupt service; corporate espionage—determine confidential processes or proprietary data.
Identifies location / recharge information for PEVs or other location-aware appliances.	*Determine Location Information* Historical PEV data, which can be used to determine range of use since last recharge. Location of active PEV charging activities, which can be used to determine the location of driver.	Utilities	Primary	Bill energy consumption to owner of the PEV; distributed energy resource management; emergency response.
		Insurance Companies	Secondary	Determine premiums based on driving habits and recharge location.
		Marketers		Profile and market based on driving habits and PEV condition.
		Private Investigators Law Enforcement/ Agencies		Investigations; locating or creating tracking histories for persons of interest.
		Civil Litigation		Determine when someone was home or at a different location.
		PEV Lessor		Verify a lessee's compliance regarding the mileage of a lease agreement.
Identifies individual meters or consumer-owned equipment and	*Identify Household Appliances* Identifying information (such as a MAC address); directly reported usage information provided by	Utilities	Primary	Load monitoring and forecasting; efficiency analysis and monitoring; reliability; demand response; distributed energy resource management; emergency response.

[63] For example, there were numerous news stories about the amount of electricity used by Al Gore's Tennessee home. *See* e.g., "Gore's High Energy-Use Home Target of Critical Report," Fox News, Feb. 28, 2007, available at http://www.foxnews.com/story/0,2933,254908,00.html.

[64] Sudden changes in when residents are home could indicate the loss of a job. Erratic sleep patterns could indicate possible stress and increased likelihood of job loss. *See e.g.*, Charles Duhigg, "What Does Your Credit-Card Company Know About You?" NY Times Mag., May 17, 2009 MM40, available at http://www.nytimes.com/2009/05/17/magazine/17credit-t.html.

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
capabilities.	"Smart" appliances. Data revealed from compromised smart meter, HAN, or other appliance.	Edge Services		Efficiency analysis and monitoring; broadcasting appliance use to social media.
		Insurance Companies	Secondary	Make claim adjustments (e.g., determine if claimant actually owned appliances that were claimed to have been destroyed by house fire); determine or modify premiums based upon the presence of appliances that might indicate increased risk; identify activities that might change risk profiles.
		Marketers		Profile for targeted advertisements based upon owned and unowned appliances or activities indicated by appliance use.
		Law Enforcement		Substantiate energy usage that may indicate illegal activity; identify activities on premises.
		Civil Litigation		Identify property; identify activities on premises.
		Criminals & Other Unauthorized Users	Illicit	Identify what assets may be present to target for theft; disrupt operation of appliances or electric service; introduce a virus or other attack to collect personal information or disrupt service; compromise smart meters to steal energy.[65]

Such data might be used in ways that raise privacy concerns. For example, granular Smart Grid data may allow numerous assumptions about the health of a dwelling's resident in which some insurance companies, employers, newspapers (when regarding public figures), civil litigants, and others could be interested. Most directly, specific medical devices may be uniquely identified through serial numbers or MAC addresses, or may have unique electrical signatures; either could indicate that the resident suffers from a particular disease or condition that requires the device.[66]

[65] See Matthew Carpenter et al., "Advanced Metering Infrastructure Attack Methodology" pages 55-56 (Jan. 5, 2009), available at http://inguardians.com/pubs/AMI_Attack_Methodology.pdf (discussing how attackers could manipulate the data reported to utilities); Robert Lemos, "Hacking the Smart Grid", Tech. Rev. (Apr. 5, 2010), available at http://www.technologyreview.com/printer_friendly_article.aspx?id=24977&channel=energy&section=.

[66] Susan Lyon & John Roche, Smart Grid News, "Smart Grid Privacy Tips Part 2: Anticipate the Unanticipated" (Feb. 9, 2010), available at

More generally, inferences might be used to determine health patterns and risk. For example, the amount of time the computer or television is on could be compared to the amount of time the treadmill is used.[67] Electricity use could also reveal how much the resident sleeps and whether he gets up in the middle of the night.[68] Similarly, appliance usage data could indicate how often meals are cooked with the microwave, the stove, or not cooked at all, as well as implying the frequency of meals.[69] Many of the parties listed in the "Potential Privacy Impacts" table (Table 5-3) will not be interested in the health of the resident and will wish to use the data for purposes such as efficiency monitoring, but some parties may be interested in the behavioral assumptions Smart Grid entities could make with Smart Grid data.

5.6.2 Wireless Access to Smart Grid Meters and Secondary Devices

Future designs for some smart meters and many secondary devices (e.g., appliances and smaller devices) may incorporate wireless-enabled technology to collect and transmit energy usage information for homes or businesses.[70] Should designers and manufacturers of smart meters or secondary devices decide to incorporate wireless technology for the purpose of communicating energy usage information, then that data must be securely transmitted and have privacy protection.[71] If in the future wireless technology is used to transmit aggregate home or business energy consumption information for a unique location or dwelling, then that usage data, prior to sufficient aggregation to protect privacy, should also be protected from unauthorized use, modification, or theft.[72] There are well-known vulnerabilities related to wireless sensors and networks,[73] and breaches of wireless technology.[74] For example, "war driving" is a popular

---

http://www.SmartGridnews.com/artman/publish/Business_Policy_Regulation_News/Smart-Grid-Privacy-Tips-Part-2-Anticipate-the-Unanticipated-1873.html.

[67] Elias Quinn mentions an Alabama tax provision that requires obese state employees to pay for health insurance unless they work to reduce their body mass index. Elias Quinn, "Privacy and the New Energy Infrastructure," Feb. 2009 (draft) page 31, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731. He suggests that Smart Grid data could be used to see how often a treadmill was being used in the home.

[68] Ann Cavoukian, Jules Polonetsky, and Christopher Wolf, Privacy by Design, "SmartPrivacy For the Smart Grid: Embedding Privacy into the Design of Electricity Conservation," Nov. 2009, available at http://www.ipc.on.ca/images/Resources/pbd-smartpriv-Smart Grid.pdf (describing the types of information that could be gleaned from combining personal information with granular energy consumption data).

[69] Id. at page 11.

[70] NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, available at http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf at page 21.

[71] *See* Table 5-2 Potential Privacy Concerns and Descriptions.

[72] Data aggregation was addressed in the final HIPAA rule. *See* http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt. There may also be efficiencies that can be gained by the Smart Grid when aggregating data from transmission and processing that save money for utilities. (*See* http://portal.acm.org/citation.cfm?id=1269968). This may create a greater incentive to aggregate data. If this is the case, then proper aggregation to protect PII or sensitive data should be incorporated into the plan for data aggregation.

[73] *See*, *e.g.*, Mark F. Foley, Data Privacy and Security Issues for Advanced Metering Systems (Part 2), available at http://www.smartgridnews.com/artman/publish/industry/Data_Privacy_and_Security_Issues_for_Advanced_Metering_Systems_Part_2.html.

technique used to locate, exploit, or attack insufficiently protected wireless systems.[75] Readily available portable computing devices are used to detect signals emanating from wireless technology.

5.6.3 Commissioning, Registration, and Enrollment for Smart Devices[76]

This subsection describes a method for implementing demand response using load control through an energy management system linked to a utility or a third-party service provider offering remote energy management. As explained in section 3.7, it is possible to protect consumer privacy by implementing demand response without a direct data connection between the energy service provider and home devices.

To create a home area network, devices must, at a minimum, scan for networks to join, request admission, and exchange device parameters. This initial process is called "commissioning" and allows devices to exchange a limited amount of information (including, but not limited to, network keys, device type, device ID, and initial path) and to receive public broadcast information. This process is initiated by the "installer" powering-on the device and following the manufacturer's instruction. Once a HAN device has completed the commissioning process, it may go through an additional process called "registration."

The registration process is a further step involving "mutual authentication" and authorizing a commissioned HAN device to exchange secure information with other registered devices and with a smart energy industrial provider. Registration creates a trust relationship between the HAN device and the smart energy industrial provider and governs the rights granted to the HAN device. This process is more complex than commissioning and requires coordination between the installer and the service provider. In some jurisdictions, commissioning and registration are combined into one process called "provisioning."

The final process is "enrollment." This process is applicable only when the consumer wants to sign up their HAN device for a specific service provider program, such as a demand-response, PEV special rate, or a prepay program. In this process, the consumer selects a service provider program and grants the service provider certain rights to communicate with or control their HAN device. A HAN device must be commissioned and registered prior to initiating the enrollment process. This process requires coordination between the consumer and the service provider. Each of these processes is discrete but may be combined by a service provider in order to provide a seamless consumer experience.

At each step in this process, the consumer, utility, and third-party provider must ensure that data flows have been identified and classified, and that privacy issues are addressed throughout, from initial commissioning up through service-provider-delivered service. Since each step in the process, including commissioning, registration, and enrollment, may contain personal

---

[74] Id.

[75] *See* Matthew Bierlein, "Policing the Wireless World: Access Liability in the Open Wi-Fi Era," Ohio State Law Journal 67 (5) page 200, available at http://moritzlaw.osu.edu/lawjournal/issues/volume67/number5/bierlein.pdf.

[76] The first four paragraphs of this subsection are taken from OpenHAN v1.95; http://www.smartgridug.net/sgsystems/openhan/Shared%20Documents/OpenHAN%202.0/UCAIug%20OpenHAN%20SRS%20-%20v1.95%20clean.doc.

information, sufficient privacy protections should be in place to minimize the potential for a privacy breach.

Privacy issues that should be addressed related to the registration of these devices with third parties include:

- Determining the types of information that is involved with these registration situations;
- Controlling the connections which transmit the data to the third-party, such as wireless transmissions from home area networks;[77] and
- Determining how the registration information is used, where it is stored, and with whom it is shared.

5.6.4 Smart Grid Data Accessibility via the Public Internet

The Smart Grid has the capability to allow users to interact with their electricity usage information in innovative ways, including via the Internet. Correspondingly, the transmission or publication of Smart Grid data via the Internet raises privacy challenges. Internet communications are generally unsecure unless those publishing the information take steps to protect the content against unauthorized interception, manipulation, or other compromises. Moreover, users do not always have complete knowledge of, or control over, how their data will be used. In essence, accessing Smart Grid data over the Internet creates risks similar to those when accessing any other type of personal information over the Internet.

For example, an energy management application provider may enable electricity consumers to monitor energy usage via cell phones, personal digital devices, and social networking pages. Online applications and portals, including social networking service providers, may not provide advance notification to these vendors or to their end users about changes to privacy settings, resulting in unintended public availability of consumer energy data[78]. Discussions of risk mitigation between public and private entities can help shape practices that avoid potential unintended exposures of consumer energy data. More research is needed to fully explore the vast privacy implications.

5.6.5 Smart Grid Data Access by Third Parties

The Smart Grid may increase the frequency and detail of electricity consumption information from private homes and businesses. The electricity consumption data that is collected, retained, and transmitted over Smart Grid systems may be of interest to third parties.[79] Third parties can include legitimate businesses with agreements with energy consumers to assist them in better managing energy consumption, but can also include criminals seeking to abuse or misuse data.

There are three privacy challenges presented by third-party access to Smart Grid information—

---

[77] The other chapters within NISTIR 7628 include recommendations for securing wireless transmissions, such as those from OpenHAN networks, to Smart Grid entities, as well as to third parties.

[78] *See* http://www.cs.virginia.edu/felt/privacy/

[79] California Public Utility Commission held hearings March 17-18, 2010, to explore the potential uses of Smart Grid data and privacy threats, available at http://www.californiaprogressreport.com/site/?q=node/7574.

11. That companies representing themselves as consumer electricity management services are what they represent themselves to be;
12. What consumers are told about how their information will be used is true;[80] and
13. Third-party access to electricity usage data is being used solely for the purpose set forth in the agreement.

An effective full suite of fair information practices protections is necessary for consumer privacy enforcement.

Authorized third parties may be interested in using data collected through the Smart Grid. The real-time data streaming capabilities of the Smart Grid may be very attractive to large appliance manufacturers, marketers interested in usage information on utility or non-utility dependent small appliances, devices, or other consumer products.[81] Unauthorized third parties will likely also be interested in misusing Smart Grid data for many reasons from theft of physical property, identity theft schemes, or surveillance of residences or businesses. Companies have relied strongly upon the "Notice and Choice" model to gain consumer consent for data collection, retention, and use. The marketing materials may promote lower energy bills through better management of energy consumption. However, the details of service agreements or "click-through" agreements of services offered solely over the Internet might contain more uses for data than energy management.[82] Simple notice is not enough to assure electricity consumer privacy protection. There are particular challenges for reliance upon notice and consent in online agreements. A survey of California consumers showed that they fundamentally misunderstand their online privacy rights.[83]

---

[80] FTC, Complaint "In the Matter of SEARS HOLDING MANAGEMENT CORPORATION" Docket No. C-4264, ("3. From on or about April 2007 through on or about January 2008, SHMC disseminated or caused to be disseminated via the Internet a software application for consumers to download and install onto their computers (the "Application"). The Application was created, developed, and managed for respondent by a third-party in connection with SHMC's "My SHC Community" market research program. 4. The Application, when installed, runs in the background at all times on consumers' computers and transmits tracked information, including nearly all of the Internet behavior that occurs on those computers, to servers maintained on behalf of respondent. Information collected and transmitted includes: web browsing, filling shopping baskets, transacting business during secure sessions, completing online application forms, checking online accounts, and, through select header information, use of web-based email and instant messaging services,") available at http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

[81] Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), *available at* http://ssrn.com/abstract=1370731

[82] David Vladeck, Privacy: Where do we go from here?, Speech to the International Conference on Data Protection and Privacy Commissioners, Nov. 6, 2009, ("[The notice and consent model] may have made sense in the past where it was clear to consumers what they were consenting to, that consent was timely, and where there would be a single use or a clear use of the data. That's not the case today. Disclosures are now as long as treatises, they are written by lawyers—trained in detail and precision, not clarity—so they even sound like treatises, and like some treatises, they are difficult to comprehend if they are read at all. It is not clear today that consent today actually reflects a conscious choice by consumers,") available at http://ftc.gov/speeches/vladeck/091106dataprotection.pdf

[83] Joseph Turow, et al., Consumers Fundamentally Misunderstand the Online Advertising Marketplace, *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf

There are added complications for consent in online click-through applications or agreements because it will be difficult to assure solely through online means that the person requesting the third party energy management service is authorized to do so. For example, if application information for third party service seeks basic application information such as home address, utility account number, or name, this information would be found on a monthly bill, which is often discarded as trash. Verifying that the legitimate electricity consumer is the one requesting service may require additional steps by utilities independent of the third party service provider. In addition, users routinely click through notices. The Pew Internet and American Life Project found that 73% of users do not always read agreements, privacy statements or other disclaimers before downloading or installing programs. Further, online businesses routinely change terms of service and privacy policy without giving notice to consumers.

Third-party consumer energy use sharing agreements may cause consumers confusion regarding the source of data misuse or abuse should it occur.

5.7 MITIGATING PRIVACY CONCERNS WITHIN THE SMART GRID

Many of the concerns relating to the 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 will benefit by developing policies to determine the consumer and premises information that should be safeguarded and how that information should be retained, distributed internally, shared with third parties, and secured against breach. As noted in other parts of this report, training employees is critical to implementing this policy. Similarly, Smart Grid services recipients should be informed as to what information the organization is collecting and how that information will be used, shared, and secured. Service recipients may also need the ability to inspect collected information for accuracy and quality, as recommended in the privacy principles described in the PIA material (subsection 5.4.2).

Existing business rules, standards, laws, and regulations previously considered relevant to other sectors of the economy might, if not directly applicable, be usable as models to provide protection against the Type II areas of concern described earlier (section 5.6, Table 5-2). However, because of the current technology used for the collection of the data, Type I concerns may need to be addressed by other means.
Many of the concerns relating to Smart Grid and privacy may be addressed by limiting the information required from an operational standpoint. For example, many existing implementations of demand response use direct load control, where the utility has a communications channel to thermostats, water heaters, and other appliances at consumer premises. . Although most direct load control today is one-way, if two-way communications are implemented, the pathway from the consumer may allow granular monitoring of energy consumption by appliance. This direct monitoring may provide more accurate load management, but could also pose certain privacy risks.

There are other methods that use demand response for distributed load control where the utility or third-party energy service provider delivers pricing and energy data to a consumer Energy Management System (EMS) through a gateway. Intelligent appliances and/or the consumer EMS use this pricing and energy information to optimize energy consumption according to consumer

preferences. With the insertion of a gateway and local intelligence, any feedback to the utility could be load control results for the entire household, rather than by appliance. To mitigate privacy concerns, these results need to be averaged over a long enough time interval to prevent pattern recognition against known load profiles, as explained in subsection 5.3.6. Thus, it is possible to protect consumer privacy at a macro level by choosing a system design that minimizes frequent access to granular data from outside the consumer site.

5.7.1 Use Case Mitigation Studies

Whereas PIAs provide an excellent means of identifying privacy risks, privacy use cases can be excellent tools for determining the specific steps to take to mitigate privacy risks in ways that are reasonable for the organization, not only for mitigating risks discovered during PIAs, but also for mitigating the generally known risks involved with common business activities that involve personal information. These generally known risks can be represented by common privacy use cases. With heavy reliance upon technology and information sharing, addressing privacy risks must be part of the business model today, and consideration of privacy impacts should be part of everyday business activities. Privacy use cases can provide the engineers and architects of systems and processes the guidance and information necessary for building privacy controls into systems and processes during their daily activities. Further discussion of this need to build privacy protections into systems and processes, along with the resulting benefits, is provided within the "Privacy By Design" methodology.[84]

When the general privacy concerns have been identified, the entities within each part of the Smart Grid can then look at their associated Smart Grid business processes and technical components to determine the privacy concerns that exist within their scope of Smart Grid use and participation. Privacy use cases may be utilized to represent generalizations of specific scenarios within the Smart Grid that require interoperability between systems and Smart Grid participants in support of business processes and workflow. Through structured and repeatable analysis, business use cases can be elaborated upon as interoperability/technical privacy use cases to be implemented by the associated entities within the Smart Grid. The resulting details will allow those responsible for creating, implementing, and managing the controls that impact privacy to do so more effectively and consistently.

5.7.2 Privacy Use Case Scenarios

The privacy subgroup spent several months creating a few different methods for expanding the existing NIST collection of use cases[85] to include consideration of privacy concerns. When considering which set of fair information practices to use for creating privacy use cases, it was decided to use the OECD Privacy Guidelines for the following reasons:

- They are long-established and widely recognized;

[84] "Privacy By Design" is a set of seven high-level concepts, created by Ontario Privacy Commissioner Ann Cavoukian, for organizations to follow to help ensure they establish and build privacy controls within their business processes. See more about the Privacy By Design concepts available at http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf.

[85] See the collection of use cases the Privacy Group considered and chose representative use cases available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases.

- They are freely available; and
- They are straight-forward concepts that will be more easily and consistently utilized when building privacy controls into processes.

The larger set of amalgamated principles used to conduct the Smart Grid PIA were chosen because they better served the purposes of identifying where, within an identified system or process, the most comprehensive set of privacy concerns exist. Typically, PIAs are performed by a specific individual or specialized group within an organization, and the PIAs look at a broader scope within a system or process and go less in-depth than a privacy use case.

Privacy use cases are typically utilized by a broader community and are repeatedly used to examine a specific, narrow scope. By keeping the privacy use case process limited to one set of accepted privacy principles such as the OECD Privacy Guidelines, it will be simpler and more feasible for the privacy use cases to be consistently used and applied by the broader community.

Appendix B contains the description of the activities of the privacy subgroup for creating privacy use cases. The privacy subgroup drafted multiple privacy use cases. The following are included as examples:

1. Landlord with Tenants scenarios
2. A PEV General Registration and Enrollment Process scenario

While the privacy subgroup created a few privacy cases, work needs to continue to finish developing a more comprehensive set of privacy use cases for publication in a subsequent version of this document.

While producing the sample privacy use cases drafts, the privacy subgroup established many recommendations based upon the work that was completed. These include:

- Expanding the current collection of use cases to cover all Smart Grid entity types in addition to utilities (regulated or not) that will offer Smart Grid and smart device services;
- Including a broader list of individuals about whom the Smart Grid, smart meters, and smart devices will generate additional personal information; and
- Including within use cases, where appropriate and feasible to allow Smart Grid goals and processes to be met, a method for individuals to turn off/on certain smart meter and smart devices collection of personal information.

The work done so far on creating privacy use cases has only begun to document the functions that need to be implemented to ensure that privacy is protected in Smart Grid operations. The privacy subgroup recommends ongoing development of a comprehensive set of use cases for privacy.

5.8 SMART GRID PRIVACY SUMMARY AND RECOMMENDATIONS

5.8.1 Summary

Based upon the work and research done over the past year, the privacy subgroup reached the following conclusions:

1. The evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, and premises may create privacy risks and challenges that are not fully addressed or mitigated by existing laws and regulations with regard to energy consumption, energy generation, billing, third-party Smart Grid applications data, and other related Smart Grid data.
2. New Smart Grid technologies, particularly smart meters, smart appliances, and similar types of endpoints, may create new privacy risks and concerns that may not be addressed adequately by the existing business policies and practices of utilities and third-party Smart Grid providers.
3. Utilities and third-party Smart Grid providers need to follow recognized privacy practices in a consistent and comprehensive fashion to effectively safeguard Smart Grid personal information and consumer privacy. Existing policies should be evaluated and revised, as required.

5.8.2 Recommendations

The challenge ahead is to create a Smart Grid Privacy Principles program that individuals accept. The goal is to have individuals participate in the Smart Grid, allowing the electric sector to thrive and innovation to occur. This will only happen when effective and transparent privacy practices are consistently implemented, followed, and enforced within the Smart Grid. To create this transparency and obtain the trust of Smart Grid participants—and based on the conclusions and the details of the associated findings—recommendations were made throughout this chapter for all entities that participate within the Smart Grid. A summary listing of all these recommendations includes:

1. Conduct a PIA before making the decision to deploy and/or participate in the Smart Grid to identify risks to the personal information Smart Grid entities collect, process, store, and otherwise handle, along with determining appropriate risk mitigation activities. Smart Grid entities can refer to the methodology followed by the privacy subgroup, as described within this report, as a model for how to do their own PIAs. PIAs should be performed as follows:
   - Conduct an initial PIA to identify existing privacy risks and establish a baseline privacy posture measurement.
   - Conduct subsequent PIAs when major changes occur within the organization, systems, or applications; when new laws and regulations are put into effect that provide requirements for how Smart Grid data is used; and at any other time an event occurs that impacts how the Smart Grid entity does business, such as following an information security incident involving personal information.
2. Develop and formally document privacy policies and practices that are drawn from the full set of OECD Privacy Principles and other sectors' privacy policies, regulations and laws that may be applicable. In particular the privacy subgroup recommends the following practices based on the Principles:
   - ***Management and Accountability***. An organization should formally appoint positions and/or personnel to ensure that information security and privacy policies and practices exist and are followed. Documented requirements for regular training and

ongoing awareness activities and communications should exist and be consistently followed. Audit functions should be present to monitor all data accesses and modifications.

- ***Notice and Purpose***. An organization should provide consumers with meaningful, clear, and full notice in advance of the collection, use, retention, or sharing of energy usage data and personal information. Such notice should provide a detailed description of all purposes for which consumer data will be used, including any purposes for which affiliates and third parties will use the data. The notice should also include how long the data will be maintained by the organization and which third parties the data will be shared with. Clear, full, and accurate notice prior to data collection is essential to enabling other principles.
- ***Choice and Consent***. An organization should clearly, fully, and accurately describe the choices available to individuals, and to the extent practicable, obtain explicit approval for the collection and use of their personal information. Consumers should have the option to forgo data collection and services that are not related to the core services provided by the organization.[86]
- ***Collection and Scope***. Only personal information that is required to fulfill the stated purpose specified under the Notice and Purpose principle should be collected. Treatment of the information should conform to these privacy principles.
- ***Use and Retention***. Information should be used or disclosed only for the purpose for which it was collected and should be divulged only to those parties authorized to receive it. Personal information should be aggregated or anonymized wherever possible to limit the potential for revealing private information. Personal information should be kept only as long as is necessary to fulfill the purposes for which it was collected.
- ***Individual Access***. Organizations should provide a process whereby individuals may ask to see their corresponding personal information and to correct inaccuracies. Individuals should be informed about parties with whom personal information has been shared.
- ***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 those identified in the notice for purposes identified in the notice, or with the explicit consent of the service recipient. Unless disclosure is compelled by a subpoena, warrant, or court order, organizations should seek prior consumer approval for disclosure of consumer data to third parties.
- ***Security and Safeguards***. Personal information in all forms should be protected from loss, theft, unauthorized access, inappropriate disclosure, copying, use, or modification.

[86] For example, while they may not have a choice about collection necessary for load balancing, electricity customers should have the option to prohibit utilities from collecting information about their appliances for marketing uses.

3. Develop a comprehensive set of privacy use cases that will help utilities and third-party Smart Grid providers to rigorously track data flows and the privacy implications of collecting and using data, and help the organization to address and mitigate the associated privacy risks within common technical design and business practices.
4. Educate the public about the privacy risks within the Smart Grid and what they as consumers can do to mitigate them.
5. Share information concerning solutions to common privacy-related problems with other Smart Grid market participants.
6. Manufacturers and vendors of smart meters, smart appliances, and other types of smart devices, should collect only the energy and personal data necessary for the purposes of the smart device operations. The defaults for the collected data should be established to use and share the data only as necessary to allow the device to function as advertised.

Given these realities, findings, and recommendations, the privacy subgroup hopes that the information contained in this chapter will serve as a useful guide and reference for the wide variety of Smart Grid domain players, policymakers, and lawmakers who have, or may have in the future, have responsibility for consumer energy consumption data.

APPENDIX C
STATE LAWS – SMART GRID AND ELECTRICITY DELIVERY REGULATIONS

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	
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	
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 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

State	Code Topic and Links
	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	
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
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 § 6-109. Duty of owner, lessee, or user of equipment. § 7-306. Net energy metering. § 7-509. Electric company's authority to regulate. Title 6. High voltage lines Title 7. Gas, electric, and water companies
Massachusetts	
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

State	Code Topic and Links
	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	
Missouri	
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
Nebraska	
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	
New Mexico	
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	
North Dakota	Title 49 Public Utilities http://www.legis.nd.gov/cencode/t49.html
Ohio	Chapter 743 Utilities – Electric; Gas; Water http://codes.ohio.gov/orc/743
Oklahoma	
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	
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	
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 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 D
PRIVACY USES CASES

The privacy subgroup—

- Reviewed a large number of existing Smart Grid use cases[87];
- Identified the privacy gaps within and among those use cases;
- Developed augmented use cases for privacy, using the traditional format used by the CSWG[88], the OECD privacy principles, and Version 2.0 of the International Security, Trust & Privacy Alliance (ISTPA) Privacy Management Reference Model;[89] and
- Summarized the key findings and observations from the collection of all the privacy use cases created.

D.1 USE CASE INVENTORY, CONSOLIDATION AND GAP ANALYSIS

The privacy subgroup developed a consolidated matrix[90]of the existing uses cases, by like topic, then looked for use cases that could represent common Smart Grid scenarios involving personal information.

The use cases were selected from several existing sources, including but not limited to IntelliGrid, Electric Power Research Institute (EPRI), and Southern California Edison (SCE). Review of this collection of use cases revealed the following:

- The existing use cases relate to utilities but not to the third parties that will also be part of the Smart Grid.
- It is not clear that the current use cases include non-regulated (e.g., third parties) Smart Grid entities or services that do not operate through the smart meter. All of the use cases reviewed require registration with a regulated Smart Grid entity and operation through the smart meter. More use cases are needed to make the available set comprehensive.
- The use cases represent situations where data is captured from not only utilities, but also from smart devices, such as a HAN or a PEV using a different plug.
- All of the use cases—
    - Referred to an individual customer, even though the information collected could be from an individual, a dwelling with multiple individuals, or business other than the

[87] See the collection of use cases that the Privacy Group considered and chose representative use cases available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases.

[88] See Appendix A in Draft 2 of NISTIR 7628, available at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628Feb2010/DRAFT2_NISTIR_7628_Jan-31-2010_clean.pdf, to see how the security groups involved in this research formatted their use cases.

[89] Developed by the International Security, Trust & Privacy Alliance (ISTPA) in 2009;

[90] See the collection of use cases that the Privacy Group considered and chose representative use cases available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases.

customer paying the Smart Grid entity bill. However, information within the Smart Grid could be personal information about a tenant, a household member, a visitor, a patient, an employee that the customer may not have the authority to grant permission to collect, and so on.

- Referred to a customer and the Smart Grid entity, even though the information collected could be from multiple individuals and could go to many entities outside of the utility.

- Reviewed assumed that if the service goes "through" the Smart Grid it has to involve the utility. There is no pass-through capability that allows an individual or business entity to enter into an agreement with a third-party using Smart Grid personal information and additional personal information generated by the smart device that travels over the grid channels.

- Assume that the Smart Grid entity can know what electronic devices are on/off/running at a premise and do not address a privacy option that could be turned on/off at some level by the individual at the premise.

- None of the use cases reviewed—

  - Made mention of a privacy policy being disseminated and being agreed to by customers.

  - Specified privacy functionality.

  - Depicted a non-regulated entity (e.g., third parties) offering a service directly to an individual or business via a smart meter.

  - Specified smart devices that communicated outside of the Smart Grid, directly with the Internet or otherwise.

D.2 INCORPORATING PRIVACY INTO EXISTING SMART GRID USE CASES

Based upon the findings the privacy subgroup recommends the following guidelines for improving upon use cases to address privacy issues—

- Add on to the existing use cases by including privacy functionality to the scenarios.
- Include information within the use cases for the existence of such things as privacy policies, training, and so on as indicated within the PIA recommendations.
- Include within the use case scenarios (1) a relationship with the utility, (2) a joint relationship with the Smart Grid utility and non-regulated entity, and (3) a relationship solely with a non-regulated entity.
- Create use cases that—
  - Include third parties that will be part of the Smart Grid.

- Include privacy options where individuals within service locations can turn on and off the ability for utilities to detect electronic devices that are using energy.
- Depict a non-regulated entity offering a service directly to an individual or business via the smart meter.
- Depict scenarios that involve smart devices and other entities within the Smart Grid communicating directly with the Internet and other non-Smart Grid entities.
- Depict groups of individuals as being the customer, or individuals at service locations who are not the entities that pay for the services. (e.g., renters that pay utilities to the landlord, not the utility)
- Include the Smart Grid entity making an agreement with a third-party and the third-party making the agreement with the individual or business entity, much like the iPhone model. In this model, the individual or business entity may or may not be the customer, but may be the owner of a smart device that communicates with the smart meter.

D.3 PRIVACY USE CASE EXAMPLES

This appendix contains the details for two example privacy use cases that were identified as examples to map to the OECD Privacy Guidelines privacy protection and fair information practices model. Each of the applicable principles is noted in the steps provided with each use case.

For reference while reviewing these privacy use cases, here is a summary of the OECD Privacy Guidelines:

1. **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, compete and kept up-to-date.
3. **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except—
    - with the consent of the data subject; or
    - by the authority of law.
5. **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. **Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle**: An individual should have the right—
   a. To obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. To have communicated to him, data relating to him
      i. within a reasonable time;
      ii. at a charge, if any, that is not excessive;
      iii. in a reasonable manner; and
      iv. in a form that is readily intelligible to him;
   c. To be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and
   d. To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. **Accountability Principle**: A data controller should be accountable for complying with measures that give effect to the principles stated above.

D.4 PRIVACY USE CASE #1: LANDLORD WITH TENANTS

"Utility Use Case Landlord/Tenant enrolls in/uses/is billed by a Smart Meter Program. In this use case, the tenant has a PEV.

D.4.1 Use Case Assumptions

- The Landlord has an account with the utility for the smart meter. The Landlord pays for all electrical service at the Tenants' premises except for the PEV.
- Each Tenant associated with a Smart Meter has the right to prevent the Landlord from obtaining detailed energy usage that would depict the presence of electrical devices in the unit as this would be an invasion of privacy.
- PEV Tenant has an account with utility and electrical service at a premise served by the utility.
- PEV and utility have communications capabilities, enabled by utility provided Energy Services Communication Interface (ESCI).
- The Tenant awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.
  - The utility offers PEV programs and services for its customers and will provide the necessary support processes for enrollment, communications, and billing

  - The Vehicle manufacturer would provide information to the customer about fuel and/or emission gains of the vehicles offered and promote the utility and convenience of connecting to the grid

- Utility maintains information on all Landlord's Smart Meters and Tenant's PEVs enrolled in the PEV programs, including demand side management programs, associated PEV IDs, Landlord IDs, and premise IDs. The Landlord is permitted detail reports, only if the Tenant allows such, even though the Landlord is paying for the electricity.
- For the purposes of this use case all of the 'DEFINE' Privacy Reference Model operational requirements have been established such that the Landlord and the Tenant have only to 'SELECT' their choices.

D.4.2 Step-by-Step Breakdown

Scenario: Landlord enrolls in the Smart Meter program. Tenants provide (or not) permission for Landlord to see detailed Smart Meter Reports and the Utilities Company turns on the service

This scenario describes the enrollment and initial usage of the Smart Meter Program.

Step 0.5 - The Landlord awareness of the utility and Smart Meter programs is prompted by both the utility providers and the Smart Meter manufacturers.

Step 1 - Landlord initiates request to enroll Smart Meter(s) in a Smart Meter Program by contacting Utility and provides Landlord, Tenant and Smart Meter information (i.e. Landlord Account information, Tenant associated with Smart Meter, SM ID, etc.). [Note: Landlord uses phone, Internet, or other communications channel.]
OECD Data Quality Principle: Collection of Personal data by the Landlord should be relevant to the purposes for which it will be used as stated by the Smart Meter provider.

Step 2 - Utility authenticates Landlord, Landlord account, and Premise information, and. collects Smart Meter information including SM ID and associated Tenant information
OECD Security Safeguards Principle: Utility must ensure proper authentication procedures are followed prior to creating a new account.

Step 3 - Utility presents Landlord with Smart Meter Program information and Smart Meter Program selections.
OECD Purposes Specification Principle: The collection of personal data should be specified by the Landlord to any Tenant and the subsequent use of the data limited to the fulfillment of those purposes
OECD Openness Principle: Utility makes available information collection and use policies to Landlord.

Step 4 - Landlord selects Smart Meter Program and Service Plan, sets Smart Meter program parameters. The Landlord and Smart Meter are now enrolled in a utility Smart Meter program.

Step 4.1 - Tenant initiates request to set up Smart Meter(s) preferences by contacting Utility and provides Landlord, Tenant and Smart Meter information (i.e. Landlord Account information, Tenant associated with Smart Meter, SM ID, etc.). [Note: Tenant uses phone, Internet, or other communications channel.]
OECD Openness Principle: Utility and Landlord make available information collection and use policies to tenant.

Step 4.2 - Utility authenticates Tenant, Landlord account, and Premise information, and collects Smart Meter information including SM ID and associated Tenant information.
OECD Security Safeguards Principle: Utility must ensure proper authentication procedures are followed by Landlord and Tenant prior to collection of Smart Meter information.

Step 4.3 - Utility presents Tenant with Smart Meter Program information and Smart Meter Program selections.
OECD Purpose Specification Principle: Tenant should be informed of the purposes for which personal data are collected should be specified not later than at the time of collection and the use limited to the fulfillment of those purposes.
OECD Use Limitation Principle: Tenant personal data should not be disclosed, made available, or otherwise used for purposes other than those specified by the Tenant.

Step 4.4 - Tenant selects Smart Meter Program and Service Plan, sets Smart Meter program parameters. The Landlord, Tenant and Smart Meter are now enrolled in a utility Smart Meter program.
OECD Individual Participation Principle: Utility must ensure proper procedures are followed for collection of Smart Meter information.

Step 5 - Tenant uses electrical services at their premise location.

Step 6 - Smart Meter and Energy Services Communications Interface (ESCI) initiate a secure communications session.
OECD Security Safeguards Principle: Utility must ensure communications channel over which information will flow is appropriately secured.

Step 7 - Smart Meter ID is transmitted to ESCI.
OECD Security Safeguards Principle: Utility must ensure communications channel over which information will flow is appropriately secured.

Step 8 - ESCI maintains communication session and security between Smart Meter and Utility. ESCI transmits request for validating Smart Meter ID to Utility, includes Premise ID.
OECD Security Safeguards Principle: Same as Step 6, plus ensuring smart meter ID matches account created.

Step 9 - Utility identifies and authenticates Smart Meter ID and Premise ID.
OECD Security Safeguards Principle: Utility ensures receiving IDs are correct before beginning session.

Step 10 - Utility transmits confirmation message via ESCI to Smart Meter indicating successful binding with premise ESCI. Confirmation message includes authentication parameters for Smart Meter. [Note: Authentication parameters would include utility rate program information.]
OECD Security Safeguards Principle: Utility ensures data is safeguarded

Step 11 - Smart Meter receives confirmation message and sets authentication parameters.
OECD Security Safeguards Principle: Utility ensures data is safeguarded and only authorized access to the data is allowed

Step 12 - Smart Meter transmits via ESCI message to Utility acknowledgement of receipt of valid confirmation message and setting of authentication parameters
OECD Security Safeguards Principle: Utility ensures data is safeguarded and provides security and authentication for access to the data

Step 13 - Utility transmits message via ESCI to discover EUMD at Tenant Premise; message includes authentication parameters for EUMD. [Note: Authentication parameters would include utility rate program information (e.g. interval size, etc.).]
OECD Security Safeguards Principle: Utility ensures data is safeguarded, data is correct and sent to valid Customer (Tenant)

Step 14 - EUMD receives discovery message and sets authentication parameters.
OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 15 - EUMD transmits via ESCI message to Utility acknowledgement of receipt of valid discovery message and setting of authentication parameters
OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 16 - ESCI transmits confirmation message to PEV indicating successful communication session binding of PEV to Utility, meaning that charging can proceed according to enrolled PEV program. [Note: Authentication between Utility and Smart Meter is now complete and the Smart Meter processing can proceed according to the enrolled Smart Meter program criteria]
OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 17 - Smart Meter prepares for collection of electrical usage based on Landlord-selected preferences, Tenant-selected preferences and enrolled Smart Meter program.
OECD Data Quality Principle: Utility ensures that meter collects only personal data relevant to the purposes for which the data is to be used and be accurate, compete and kept up-to-date.
OECD Purpose Specification Principle: Utility follows Tenant preferences regarding personal data collection and the subsequent limited use

OECD Use Limitation Principle: Utility maintains process so that personal data is not disclosed, made available or otherwise used for purposes other than those specified by the Tenant

Step 18 - Utility prepares for report of electrical usage based on Landlord-selected preferences, Tenant-selected preferences and enrolled Smart Meter program.
OECD Individual Participation Principle: Data and usage collection reports should be made available to Tenant according to their preferences
OECD Accountability Principle: Utility is held accountable for complying with data security and access requirements

D.5 PRIVACY USE CASE #2: PEV GENERAL REGISTRATION AND ENROLLMENT PROCESS

Customers are interested in fueling vehicles with electricity. Electric vehicles (EV), plug-in vehicles (PEV) and plug-in hybrid vehicles (PHEV) are emerging transportation options for consumers. Electric utilities desire to support these emerging loads with electricity at "off peak" times when energy costs are low and generation and power delivery assets are underutilized. PEV manufacturers are interested in working with utilities to develop customer rates/programs which could provide consumers with an increased incentive to purchase a PEV. To enable utility customer rates/programs specifically to customers with PEVs, the utility must offer special services for these customers. These services include the ability to enroll, register, and initially setup communications between a PEV and the utility (one-time setup), the ability to repeatedly re-establish communications for each PEV charging session (repeat communications/re-binding), the ability to provide PEV charging (and other) status information to customer information channels (e.g. web, display devices), and the ability to correctly bill PEV customers according to their selected rates/programs.

The Utility may offer the Customer a PEV tariff that provides a low rate for off-peak charging and a higher rate for on-peak charging. The utility must provide services to support energy supplied to customer PEV. These services include enrollment into a PEV program, PEV communications session binding, PEV energy billing, and PEV information services. The utility will implement an enrollment system for Customers with a PEV including registration and commissioning. The utility's Energy Services Communication Interface (ESCI) allows for the establishment of a communications session (communications binding), at a premise location each time a PEV plugs in for charging. Energy supplied to the PEV is reported to the utility for billing and presentation to the Customer. Information related to utility PEV programs, energy usage, and PEV charging status/information will be made available to the Customer for viewing via a website or other customer provided display equipment. This use case covers general information for the following five scenarios:

1. Enrollment Process to Time of Use (TOU) Program
2. Enrollment Process to Direct Load/Device Control (DDC) Program
3. Enrollment Process to Real Time Pricing (RTP) or Hourly/Periodic Pricing Program
4. Enrollment Process to Critical Peak Pricing (CPP) or Hourly/Periodic Pricing Program
5. Enrollment Process to Active Load Management Program

- These programs apply to routine or prearranged customer, vehicle usage and charging events.
- It is expected that the enrollment process would identify the customers normal charging pattern, specific details on the vehicle(s) operated that could be matched with anticipated load info to predict minimum effects on the grid.

D.5.1 Use Case Assumptions

- PEV Customer has an account with utility and electrical service at a premise served by the utility.
- PEV and utility have communications capabilities, enabled by utility provided Energy Services Communication Interface (ESCI).
- The customer awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.
  - The utility offers PEV programs and services for its customers and will provide the necessary support processes for enrollment, communications, and billing
  - The Vehicle manufacturers would provide information to the customer about fuel and/or emission gains of the vehicles offered and promote the utility and convenience of connecting to the grid
- Utility maintains information on all Customers and PEVs enrolled in the PEV programs, including demand side management programs, associated PEV IDs, customer IDs, and premise IDs
- EUMD function can be inclusively located anywhere in a zone from the PEV and the branch circuit panel connection.
- In the absence or failure of PEV-utility communications, or if PEV ID validation fails, PEV charging will always proceed; however, without the incentive rates and with all energy charges accruing to the premise customer according to the premise customer's default rate/service plan.
- The actual PEV charging processes, including scenarios for intra-and inter- utility roaming, are covered in use case P2.
- End Use Measurement Device (EUMD) is always available for PEV charging. If not available, charging will proceed without incentive rates and with all energy charges accruing to the premise customer. This may or may not prevent certain charging status indicators / metrics being available to customer for presentation/display purposes.
- EUMD function can be inclusively located anywhere in a zone from the PEV and the branch circuit panel connection.

To allow for possibility of the EUMD being a part of/within the PEV, PEV is a sub-meter to the primary utility billing meter at any premise (as opposed to being a separate service account with dual meter socket adapter)

The PEV and Utility will communicate to implement one or more the previously described Utility programs

D.5.2 Step by Step Breakdown

Scenario: Customer enrolls in PEV program (Basic Enrollment) and completes initial setup for PEV– Utilities communications

This scenario describes the most common sequence (basic process) of the utility enrolling a PEV customer into a utility program/ service specifically for customers with PEVs. As described in the main Narrative section, the customer is enrolling in a PEV program/service that may provide for the opportunity to fuel a vehicle at a lower cost during off-peak periods based on one of the utility programs enumerated in the main Narrative section. This scenario involves both enrollment of the PEV and steps needed to establish an initial communications session with the utility.

Step 0.5 - The customer awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.

Step 1 - Customer initiates request to enroll PEV in a PEV Program by contacting Utility and provides Customer and PEV information (i.e. Customer Account information, PEV ID, etc.). [Note: Customer uses phone, Internet, or other communications channel. Preference for PEV is PEV VIN #]
OECD Collection Limitation Principle: Utility collects data by action of the customer

Step 2 - Utility authenticates Customer, Customer account, and Premise information, and collects PEV information including PEV ID.
OECD Security Safeguards Principle: Customer Account data authenticated by Utility to establish identification for PEV

Step 3 - Utility presents Customer with PEV Program information and PEV Program selections.
OECD Purpose Specification Principle: Utility communications to Customer regarding data collection practices

Step 4 - Customer selects PEV Program and Service Plan, sets PEV program parameters (e.g., guest charging, allow roaming, etc.). The Customer and PEV are now enrolled in a utility PEV program.
OECD Individual Participation Principle: Customer confirms data collection arrangements with Utility

Step 5 - Customer connects at their premise location. [Note: The connection could be using either EVSE corset or Premise EVSE. In this scenario we will consider that PEV is connected through EVSE cordset]

Step 6 - PEV and Energy Services Communications Interface (ESCI) initiate a secure communications session. [Note: Implementation could have PEV or ESCI as initiator of session.]
OECD Security Safeguards Principle: Utility establishes secure interface and authenticates session for data collection

Step 7 - PEV ID is transmitted to ESCI. [Note: Unique PEV ID will ultimately support portability of charging, among other purposes.
OECD Security Safeguard Principle: Utility collects Customer data through PEV identification using secure interface and by rearranged process and procedure to secure the data

Step 8 - ESCI maintains communication session and security between PEV and Utility. ESCI transmits request for validating PEV ID to Utility, includes Premise ID.
OECD Security Safeguard Principle: Utility maintains secure interface to transmit data it has collected. Data is also validated according to Utility procedures

Step 9 - Utility identifies and authenticates PEV ID and Premise ID. [Note: PEV binds with utility]
OECD Data Quality Principle: Utility confirms identity and authenticates data per collection practices

Step 10 - Utility transmits confirmation message via ESCI to PEV indicating successful binding with premise ESCI. Confirmation message includes authentication parameters for PEV.
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission

Step 11 - PEV receives confirmation message and sets authentication parameters.
OECD Security Safeguards Principle: Utility confirms data transmission

Step 12 - PEV transmits via ESCI message to Utility acknowledgement of receipt of valid confirmation message and setting of authentication parameters.
OECD Security Safeguards Principle: Utility through secure interface confirms data transmission

Step 13 - Utility transmits message via ESCI to discover EUMD at Customer Premise; message includes authentication parameters for EUMD. [Note: Authentication parameters would include utility rate program information (e.g. interval size, etc.).]
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission

Step 14 - EUMD receives discovery message and sets authentication parameters.
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission

Step 15 - EUMD transmits via ESCI message to Utility acknowledgement of receipt of valid discovery message and setting of authentication parameters.
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission

Step 16 - ESCI transmits confirmation message to PEV indicating successful communication session binding of PEV to Utility, meaning that charging can proceed according to enrolled PEV program. [Note: Authentication between Utility and PEV is now complete and charging can proceed according to the enrolled PEV program criteria]

OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission using validation process according to Customer preferences

Step 17 - PEV prepares for charging based on Customer-selected preferences and enrolled PEV program. Charging may be delayed based upon Customer preferences or grid reliability criteria (e.g., off-peak economy charging, demand response event underway, short, randomized charging delay to promote grid stability, etc.)
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission using validation process according to Customer preferences

APPENDIX E
PRIVACY RELATED DEFINITIONS

Because "privacy" and associated terms mean many different things to different audiences, it is important to establish some definitions for the terms used within this chapter to create a common base of understanding for their use. The energy-specific terms are defined within Appendix I. The definitions of the terms related to privacy, as they are used within this chapter, follow.

E.1 PRIVACY IMPACT ASSESSMENT

A privacy impact assessment (PIA) is a structured, repeatable, type of analysis of how information relating to or about individuals, or groups of individuals, is handled. A report, similar to that of an audit report, is generated to describe the types of privacy risks discovered based upon each privacy category, to document the findings, and then to provide recommendations for mitigating the privacy risk findings. Common goals of a PIA include:

1. Determining if the information handling and use within the identified scope complies with legal, regulatory, and policy requirements regarding privacy;
2. Determining the risks and effects of collecting, maintaining, and disseminating information in identifiable, or clear text, form in an electronic information system or groups of systems; and
3. Examining and evaluating the protections and alternative processes for handling information to mitigate the identified potential privacy risks.

E.2 PERSONAL INFORMATION

"Personal information" is a broad term that includes personally identifiable information (PII), in addition to other types of information. Personal information may reveal information about, or describe, an individual, or group of individuals, such as a family, household, or residence. This information includes, but is not limited to, such information as name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, statements made by, or attributed to, the individual, and utility usage information, all of which could be used to impact privacy.

Personal information includes not only PII, as defined below, but also information that may not be specifically covered within existing laws, regulations or industry standards, but does have recognized needs for privacy protections. For example, a social networking site may reveal information about energy usage or creation.

Personal information within the Smart Grid includes, but is not be limited to, information that reveals details, either explicitly or implicitly, about a specific individual's or specific group's type of premises and energy use activities. This is expanded beyond the normal "individual" component because there could be negative privacy impacts for all individuals within one dwelling or building structure. This can include items such as energy use patterns, characteristics related to energy consumption through smart appliances, and other types of activities. The energy use pattern could be considered unique to a household or premises similar to how a fingerprint or DNA is unique to an individual.

Personal information also includes energy use patterns that identify specific appliances or devices that may indicate a medical problem of a household member or visitor; the inappropriate use of an employer issued device to an employee that is a household member or visitor; the use of a forbidden appliance in a rented household. Smart appliances and devices will create additional information that may reveal a significant amount of additional personal information about an individual, such as what food they eat, how much they exercise and detailed physical information. This would also become a privacy issue in a university, office setting, healthcare facility and so on.

E.3 PERSONALLY IDENTIFIABLE INFORMATION (PII)

"PII" is information that has been defined within existing laws, regulations and industry standards, as those specific types of information items that can be tied to a unique individual in certain situations and has some current form of legal protection as a result. For example, the U.S. Health Insurance Portability and Accountability Act requires the following types of individually identifiable information to be safeguarded:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers (including energy bill account numbers, credit card numbers, and so on)
- Certificate and license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device Identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images;
- Any other unique identifying number, characteristic, or code

With the exception of those terms specifically naming energy, the above are the items defined within the Health Insurance Portability and Accountability Act (*HIPAA*) of 1996, which arguably

has the widest definition of PII within the existing U.S. federal regulations. More identifiers may be added to the list as the Smart Grid evolves and as regulations change.

E.4 COMPOSITE PERSONAL INFORMATION

"Composite personal information" is non-personal information items that, when combined with certain other non-personal information items, can become personal information. In other words, it is the aggregation or combination of non-personal information that reveals insights into personal lives, characteristics and activities, thus forming personal information. Consider a zip code, gender, and birth year. If you look at each of these separately, it would be hard to say you can link each of them to a specific individual. However, if you look at the three items in combination, you may be able to identify a specific individual, particularly in more sparsely populated geographic locations.

E.5 PRIVATE INFORMATION

"Private information" is information that is associated with individuals or groups of individuals, which could reveal details of their lives or other characteristics that could impact them. Private information is not necessarily information that, on its own, is linked to individuals directly.

Private information is typically a classification of information that individuals use for themselves. It is a broad and general term that is more ambiguously used than other privacy terms. For example, the combination to a bank safety deposit lock is private, but the combination number itself does not point to any specific individual. As another example, some individuals consider how they voted in presidential elections to be private information that they do not want any others know. Other individuals, however, communicate how they voted on bumper stickers for the world to see because they have determined that, for them, it is not private information.

Individuals often consider PII to be a type of private information, and personal information could also be private information. For utilities, market data that includes information about a negotiated price for a customer is likely considered by the customer to be private information; they may not want their friends, neighbors or the general public to see this information. Smart device data from within consumer dwellings could also be a type of private information. Private information could cause harm to the associated individuals or groups if misused or accessed by those who do not have a business need. "Private information" is a term used by individuals that indicates information they have determined they do not want others to know, and is not a term used as a data classification type by business organizations.

E.6 CONFIDENTIAL INFORMATION

"Confidential information" is information for which access should be limited to only those with a business need to know, and that could result in compromise to a system, data file, application, or other business function if inappropriately shared. Confidential information is a common term used by businesses as one of their data classification labels. For example, the formula for Coca-Cola is confidential. The plans for a new type of wind turbine, that have not yet been publicized, are confidential.

Market data that does not include customer specific details may be confidential. Many types of personal information can also fall within the "Confidential Information" data classification label. Information can be confidential at one point in the information lifecycle, and then become public at another point in the lifecycle. Information that an organization does not want shared outside of

their organization, which they consider to be proprietary, is considered to be confidential information. Confidential information must have appropriate safeguards applied to ensure only those with a business need to fulfill their job responsibilities can access the information.

E.7 INDIVIDUAL

Any specific person.

E.8 SMART GRID ENTITY

An entity that participates within the Smart Grid and that collects, stores, uses, shares, transfers across borders, or retains Smart Grid data.

NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

The Smart Grid Interoperability Panel – Cyber Security Working Group

August 2010

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

NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

The Smart Grid Interoperability Panel–Cyber Security Working Group

August 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 (IT). 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 National Institute of Standards and Technology Interagency Report (NISTIR) 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, vol. 3
219 pages (August 2010)

ACKNOWLEDGMENTS

This report was developed by members of the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP-CSWG), formerly the Cyber Security Coordination Task Group (CSCTG), and during its development was chaired by Annabelle Lee of the Federal Energy Regulatory Commission (FERC), formerly of NIST. The CSWG is now chaired by Marianne Swanson (NIST). Alan Greenberg (Boeing), Dave Dalva (Cisco Systems), and Bill Hunteman (Department of Energy) are the vice chairs. Mark Enstrom (Neustar) is the secretary. Tanya Brewer of NIST is the lead editor of this report. The members of the SGIP-CSWG have extensive technical expertise and knowledge to address the cyber security needs of the Smart Grid. The dedication and commitment of all these individuals over the past year and a half is significant. In addition, appreciation is extended to the various organizations that have committed these resources to supporting this endeavor. Members of the SGIP-CSWG and the working groups of the SGIP-CSWG are listed in Appendix J of this report.

In addition, acknowledgement is extended to the NIST Smart Grid Team, consisting of staff in the NIST Smart Grid Office and several of NIST's Laboratories. Under the leadership of Dr. George Arnold, National Coordinator for Smart Grid Interoperability, their ongoing contribution and support of the CSWG efforts have been instrumental to the success of this report.

Additional thanks are extended to Diana Johnson (Boeing) and Liz Lennon (NIST) for their superb technical editing of this report. Their expertise, patience, and dedication were critical in producing a quality report. Thanks are also extended to Victoria Yan (Booz Allen Hamilton). Her enthusiasm and willingness to jump in with both feet are really appreciated.

Finally, acknowledgment is extended to all the other individuals who have contributed their time and knowledge to ensure this report addresses the security needs of the Smart Grid.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

OVERVIEW AND REPORT ORGANIZATION

REPORT OVERVIEW

Version 1.0 (V1.0) of NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, is the Smart Grid Interoperability Panel—Cyber Security Working Group's (SGIP-CSWG's) report for individuals and organizations who will be addressing cyber security for Smart Grid systems. This includes, for example, vendors, manufacturers, utilities, system operators, researchers, and network specialists; and individuals and organizations representing the IT, telecommunications, and electric sectors. This report assumes readers have a basic knowledge of the electric sector and a basic understanding of cyber security.

AUDIENCE

This report is intended for a variety of organizations that may have overlapping and different perspectives and objectives for the Smart Grid. For example—

- *Utilities/asset owners/service providers* may use this report as guidance for a specific Smart Grid information system implementation;
- *Industry/Smart Grid vendors* may base product design and development, and implementation techniques on the guidance included in this report;
- *Academia* may identify research and development topics based on gaps in technical areas related to the functional, reliability, security, and scalability requirements of the Smart Grid; and
- *Regulators/policy makers* may use this report as guidance to inform decisions and positions, ensuring that they are aligned with appropriate power system and cyber security needs.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
  - 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* includes a high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. The chapter also includes individual diagrams for each of the 22 logical interface categories. This architecture focuses on a short-term view (1–3 years) of the Smart Grid.
  - Chapter 3 – *High Level Security Requirements* specifies the high level security requirements for the Smart Grid for each of the 22 logical interface categories included in Chapter 2.

  - Chapter 4 – *Cryptography and Key Management* identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.
  - Appendix A – *Crosswalk of Cyber Security Documents*
  - Appendix B – *Example Security Technologies and Procedures to Meet the High Level Security Requirements*
- Volume 2 – Privacy and the Smart Grid
  - Chapter 5 – *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 that may occur as new capabilities are included in the Smart Grid.
  - Appendix C – *State Laws – Smart Grid and Electricity Delivery*
  - Appendix D – *Privacy Use Cases*
  - Appendix E – *Privacy Related Definitions*
- Volume 3 – Supportive Analyses and References
  - Chapter 6 – *Vulnerability Classes* includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.
  - Chapter 7 – *Bottom-Up Security Analysis of the Smart Grid* identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.
  - Chapter 8 – *Research and Development Themes for Cyber Security in the Smart Grid* 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.
  - Chapter 9 – *Overview of the Standards Review* includes an overview of the process that is being used to assess standards against the high level security requirements included in this report.
  - Chapter 10 – *Key Power System Use Cases for Security Requirements* identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.
  - Appendix F – *Logical Architecture and Interfaces of the Smart Grid*
  - Appendix G – *Analysis Matrix of Interface Categories*
  - Appendix H – *Mappings to the High Level Security Requirements*
  - Appendix I – *Glossary and Acronyms*
  - Appendix J – *SGIP-CSWG Membership*

CHAPTER SIX
VULNERABILITY CLASSES

6.1 INTRODUCTION

This section is intended to be used by those responsible for designing, implementing, operating or procuring some part of the electric grid. It contains a list of five classes of potential vulnerabilities with descriptions of specific areas that can make an organization vulnerable as well as the possible impacts to an organization should the vulnerability be exercised. For the purpose of this document, a vulnerability class is a category of weakness which could adversely impact the operation of the electric grid. 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. This document contains a number of possible vulnerabilities, identified by management, operational and technical categories. It is best used as a stimulus for detailed risk analysis of real or proposed systems, and while it was created from many sources of vulnerability information, including NIST 800-82, *Guide to Industrial Control Systems Security,* and 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Open Web Application Security Project (OWASP) vulnerabilities, National Vulnerability Database Common Weakness Enumeration (CWE) vulnerabilities, attack documentation from Idaho National Laboratory (INL), input provided by the NIST CSWG Bottom-Up group, and the North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) standards, it is just a starting point for more detailed vulnerability identification in future CSWG work efforts.

6.2 PEOPLE, POLICY & PROCEDURE

Policies and procedures are the documented mechanisms by which an organization operates, and *people* are trained to follow them. Policies and procedures lay the groundwork for how the organization will operate. This section discusses cases where a failure in, lack of, or deficiency in policies and procedures can lead to security risks for the organization. An organization's policies and procedures are often the final protective or mitigating control against security breaches, and those policies and procedures should be examined closely to ensure that they are consistent with both the inherent business objectives and with secure operations.

6.2.1 Training

This category of vulnerabilities is related to personnel security awareness training associated with implementing, maintaining, and operating systems.

6.2.1.1 Insufficiently 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 assets one is responsible for.

Through training, everyone in the organization gets a clear understanding of the importance of cyber security, but more importantly everyone begins to understand the role they play and the importance of each role in supporting security.

Examples

- Freely releasing information of someone's status, i.e. away on vacation, not in today, etc.,
- Opening emails and attachments from unknown sources,
- Posting passwords for all to see,
- Allowing people to dumpster-dive without alerting security, and
- Failure to notice inappropriate or suspicious network cables/devices outside the building.

Potential Impact:

Social engineering is used in acquiring as much information as possible about people, organizations and organizational operations. Insufficiently trained personnel may inadvertently provide the visibility, knowledge and opportunity to execute a successful attack.

6.2.1.2 Inadequate Security Training and Awareness Program

Description

An adequate security awareness program is a key element of an organization's policy framework to guard against vulnerabilities introduced by insufficiently trained personnel. Such programs highlight the need for a continuous retraining effort over some identified period of time. The security profile will always be changing and so will the need for new procedures, new technologies, and reinforcement of the importance of the cyber security program.

Potential Impact

An inadequate trained workforce will not be aware of the policies and procedures necessary to secure organizational information and equipment, resulting in the potential for weaknesses to be exploited for example:

- Inserting malicious USB sticks found in the parking lot into machines with access to control-systems providing attackers control over the control systems.
- Holding the door for potential attackers carrying a big box entering a "secured premise", allowing them unauthorized access and physical proximity to critical / control systems.
- Surfing porn sites (which often includes 0-day exploits and compromise workstations with bots or worms.
- Failing to respond to someone capturing wireless network traffic on the front lawn or parked in the guest parking lot, and
- Lack of care with id badges and credentials which can be leveraged to gain partial or complete access to critical machines.

6.2.2 Policy & Procedure

6.2.2.1 Insufficient Identity Validation, Background Checks

Description

Identity validation/background checks are based on the individual's area of responsibility and the type of information authorized to access. The more sensitive information available to an individual, the deeper and more detailed the validation and checking process should be.

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

Potential Impact

The human factor must always be considered the weakest element within any security posture, thus identity validation and background checks are measures that are imperative in managing this risk. As the amount and sensitivity of the information one is given responsibility for increases, consideration should be given to requiring separation of duties to ensure that no one individual is given "the keys to the kingdom."

6.2.2.2 Inadequate Security Policy

Description

Security policies must be structured with several key elements, must be well understood, must embody a practical approach, must be well practiced and monitored, and must be enforceable.

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

Potential Impact

Vulnerabilities are often introduced due to inadequate policies or the lack of policies. Policies need to drive operating requirements and procedures.

6.2.2.3 Inadequate Privacy Policy

Description

A privacy policy should be established that documents the necessity of protecting private/personal information to ensure that data is not exposed or shared unnecessarily.

Potential Impact

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

6.2.2.4 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.

6.2.2.5 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, and
- Making a change to network configuration and failing to document that change.

Potential Impact

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

6.2.2.6 Unnecessary System Access

Description

As a matter of policy, it needs to be very clear that system access and information is granted only on a need basis. System access needs to be managed, monitored, and enforced based on the individual's access requirements and the level of impact that uncontrolled access could have on an organization.

Potential Impact

System access that is not managed can result in personnel obtaining, changing or deleting information they are no longer authorized to access as well as:

- Administrators with false assumptions of what actions any one user may be capable.
- One user (or many individual users) may have sufficient access to cause complete failure or large portions of the electric grid.
- Inability to prove responsibility for a given action or hold a party accountable.
- Accidental disruption of service by untrained individuals, and
- Raised value for credentials of seemingly insignificant personnel.

6.2.3 Risk Management

Deficiencies in a risk management program can lead to vulnerabilities throughout the organization. A well documented and implemented risk management program that encompasses the organization-wide level, mission level and the technical level will provide an in depth defense against many potential vulnerabilities.

6.2.3.1 Inadequate Periodic Security Audits

Description

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

Potential Impact

The audit process is the only true measure by which it is possible to continuously evaluate the status of the implemented security program in terms of conformance to policy, determine whether there is a need to enhance policies and procedures, and evaluate the robustness of the implemented security technologies.

6.2.3.2 Inadequate Security Oversight by Management

Description

An overall security program requires the crossing of many organization operating groups, has impact on many business areas, and requires an element of human recourses and legal involvement. Without senior management oversight/ownership, it is very difficult to maintain a successful security program and posture. A significant challenge can exist in establishing senior management oversight at the executive level within an organization.

Potential Impact

A lack of clear senior management ownership of a security program makes it almost impossible to enforce the provisions of the program in the event of a policy being compromised or abused.

6.2.3.3 Inadequate Continuity of Operations or Disaster Recovery Plan

Description

It is essential to ensure within the various plant/system disaster recovery plans that are in place that an associated cyber contingency plan and cyber security incident response plan is developed. Each plant/system disaster recovery plan should highlight the need to determine if the disaster was created by or related to a cyber security incident. If such is the case, then part of the recovery process must be to ensure cyber incident recovery and contingency activities are implemented. This means taking added steps like validating backups, ensuring devices being recovered are clean before installing the backups, incident reporting, etc.

Potential Impact

An inadequate continuity of operations or disaster recovery plan could result in longer than necessary recovery from a possible plant or operational outage.

6.2.3.4 Inadequate Risk Assessment Process

Description

A documented risk assessment process that includes consideration of business objectives, the impact to the organization if vulnerabilities are exploited, and the determination by senior management of risk acceptance is necessary to ensure proper evaluation of risk.

Potential Impact

Lack or misapplication of adequate risk assessment processes can lead to poor decisions based on inadequate understanding of actual risk.

6.2.3.5 Inadequate Incident Response Process

Description

An incident response process is required to ensure proper notification, response, and recovery 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 risk exposure.

6.3 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. These errors and oversights are discovered and reported as vulnerability instances in platform software and firmware. Discovery and reporting of vulnerability instances occurs continuously and the Common Vulnerability and Exposures (CVE) specification establishes a common identifier for known vulnerability instances. [§6.6-5] The Common Weakness Enumeration (CWE) [§6.6-4] and the Vulnerability Categories defined by OWASP [§6.6-1] are two taxonomies which provide descriptions of common errors or oversights that can result in vulnerability instances. Using the CWE and OWASP taxonomies as a guide this subsection describes classes and subclasses of vulnerabilities in platform software and firmware[1].

[1] The OWASP names are generally used with the exact or closest CWE-ID(s) match in parentheses. The mappings are informational only and are not to be considered authoritative.

6.3.1 Software Development

Applications being developed for use in the Smart Grid should make use of a secure software development life cycle (SDLC). Vulnerabilities in this category can arise from a lack of oversight in this area, leading to poor code implementation, leading to vulnerability.

6.3.1.1 Code Quality Vulnerability (CWE-398)

Description

"Poor code quality," states OWASP, "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." [§6.6-1]

Examples

- Double free() errors (CWE-415),
- Failure to follow guideline/specification (CWE-573),
- Leftover debug code (CWE-489),
- Memory leak (CWE-401),
- Null dereference (CWE-476, CWE-690),
- Poor logging practice,
- Portability flaw (CWE-474, CWE-589),
- Undefined behavior (CWE-475),
- Uninitialized variable (CWE-457),
- Unreleased resource (CWE-404),
- Unsafe mobile code (CWE-490),
- Use of obsolete methods (CWE-477),
- Using freed memory (CWE-416), and
- Buffer overflow (CWE-120).

6.3.1.2 Authentication Vulnerability (CWE-287)

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 [§6.6-1]

- Allowing password aging (CWE-263),
- Authentication bypass via assumed-immutable data (CWE-302),

- Empty string password (CWE-258),
- Failure to drop privileges when reasonable (CWE-271),
- Hard-coded password (CWE-259),
- Not allowing password aging (CWE-262),
- Often misused: authentication (CWE-247),
- Reflection attack in an auth protocol (CWE-301),
- Unsafe mobile code (CWE-490),
- Using password systems (CWE-309),
- Using referrer field for authentication or authorization (CWE-293), and
- Using single-factor authentication (CWE-308).

Potential Impact

Access granted without official permission

6.3.1.3 Authorization Vulnerability (CWE-284)

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

- Access control enforced by presentation layer (CWE-602, CWE-425),
- File access race condition: time-of-check, time-of-use (TOCTOU) (CWE-367),
- Least privilege violation (CWE-272),
- Often misused: privilege management (CWE-250),
- Using referrer field for authentication or authorization (CWE-293),
- Insecure direct object references (CWE-639, CWE-22), and
- Failure to restrict universal resource locator (URL) access (CWE-425, CWE-288).

6.3.1.4 Cryptographic Vulnerability (CWE-310)

Description

Cryptography is the use of mathematical principles and their implementations 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 that allow an attacker to view, modify, or forge encrypted data or impersonate another party through digital signature abuse.

Examples

- Failure to encrypt data (CWE-311),
- Insecure Randomness (CWE-330),
- Insufficient Entropy (CWE-332),
- Insufficient Session-ID Length (CWE-6),
- Key exchange without entity authentication (CWE-322),
- Non-cryptographic pseudo-random number generator (CWE-338),
- Not using a random initialization vector with cipher block chaining mode (CWE-329),
- PRNG Seed Error (CWE-335),
- Password Management: Weak Cryptography (CWE-261),
- Reusing a nonce, key pair in encryption (CWE-323),
- Testing for SSL-TLS (OWASP-CM-001) (CWE-326),
- Use of hard-coded cryptographic key (CWE-321),
- Using a broken or risky cryptographic algorithm (CWE-327), and
- Using a key past its expiration date (CWE-324).

6.3.1.5 Environmental Vulnerability (CWE-2)

Description

"This category," states OWASP, "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." [§6.6-1]

Examples

- ASP.NET misconfigurations (CWE-10),
- Empty string password (CWE-258),
- Failure of true random number generator (CWE-333),
- Information leak through class cloning (CWE-498),
- Information leak through serialization (CWE-499),
- Insecure compiler optimization (CWE-14),
- Insecure transport (CWE-319, CWE-5),
- Insufficient session-ID length (CWE-6),
- Insufficient entropy in pseudo-random number generator (CWE-332),
- J2EE misconfiguration: unsafe bean declaration (CWE-8),

- Missing error handling (CWE-7),
- Publicizing of private data when using inner classes (CWE-492),
- Relative path library search (CWE-428),
- Reliance on data layout (CWE-188),
- Relying on package-level scope (CWE-487),
- Resource exhaustion (CWE-400), and
- Trust of system event data (CWE-360).

6.3.1.6 Error Handling Vulnerability (CWE-703)

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 (CWE-10),
- Catch NullPointerException (CWE-395),
- Empty catch block (CWE-600),
- Improper cleanup on thrown exception (CWE-460),
- Improper error handling (CWE-390),
- Information leakage (CWE-200),
- Missing error handling (CWE-7),
- Often misused: exception handling (CWE-248),
- Overly-broad catch block (CWE-396),
- Overly-broad throws declaration (CWE-397),
- Return inside finally block (CWE-584),
- Uncaught exception (CWE-248),
- Unchecked error condition (CWE-391), and
- Unrestricted File Upload (CWE-434).

6.3.1.7 General Logic Error (CWE-691)

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 (CWE-464),
- Assigning instead of comparing (CWE-481),
- Comparing instead of assigning (CWE-482),
- Deletion of data-structure sentinel (CWE-463),
- Duplicate key in associative list (CWE-462),
- Failure to check whether privileges were dropped successfully (CWE-273),
- Failure to de-allocate data (CWE-401),
- Failure to provide confidentiality for stored data (CWE-493),
- Guessed or visible temporary file (CWE-379),
- Improper cleanup on thrown exception (CWE-460),
- Improper error handling (CWE-390),
- Improper temp file opening (CWE-378),
- Incorrect block delimitation (CWE-483),
- Misinterpreted function return value (CWE-253),
- Missing parameter (CWE-234),
- Omitted break statement (CWE-484),
- Passing mutable objects to an untrusted method (CWE-375),
- Symbolic name not mapping to correct object (CWE-386),
- Truncation error (CWE-197),
- Undefined Behavior (CWE-475),
- Uninitialized Variable (CWE-457),
- Unintentional pointer scaling (CWE-468),
- Use of sizeof() on a pointer type (CWE-467), and
- Using the wrong operator (CWE-480).

6.3.1.8 Business logic Vulnerability

Description

Business logic vulnerabilities occur when the legitimate processing flow of an application is used in a way that results in an unintended consequence. Discovery and testing of this vulnerability class tends to be specific to an application under analysis and require detailed knowledge of the business process. Additional information on this vulnerability may be found at [§6.6-10]

Examples

- Purchase orders are not processed before midnight,
- Written authorization is not on file before web access is granted, and
- Transactions in excess of $2000 are not reviewed by a person.

6.3.1.9 Input and Output Validation (CWE-20 AND CWE-116)

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". Output validation is encoding or escaping data during the preparation of a structured message for communication with another component. Improper output validation can allow attackers to change or replace the commands sent to other components.

Examples

- Buffer overflow (CWE-120),
- Format string (CWE-134),
- Improper data validation (CWE-102, CWE-103, CWE-104, CWE-105, CWE-106, CWE-107, CWE-108, CWE-109, CWE-110),
- Log forging (CWE-117),
- Missing XML validation (CWE-112),
- Process control (CWE-114),
- String termination error (CWE-158),
- Unchecked return value: missing check against null (CWE-690, CWE-252),
- Unsafe Java Native Interface (JNI) (CWE-111),
- Unsafe reflection (CWE-470),
- Validation performed in client (CWE-602),
- Unvalidated redirects and forwards (CWE-819), and
- Improper Neutralization of HTTP Headers for Scripting Syntax (CWE-664).

6.3.1.10 Logging and Auditing Vulnerability (CWE-778 and CWE-779)

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 (CWE-464),
- Information leakage (CWE-200),
- Log forging (CWE-117),
- Log injection (CWE-117),
- Poor logging practice, and
- Cross-site scripting via HTML log-viewers (CWE-79, CWE-117).

6.3.1.11 Password Management Vulnerability (CWE-255)

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

- Empty string password (CWE-258),
- Hard-coded password (CWE-259),
- Not allowing password aging (CWE-262),
- Password management: hardcoded password (CWE-259),
- Password management: weak cryptography (CWE-261),
- Password plaintext storage (CWE-256),
- Password in configuration file (CWE-260), and
- Using password systems (CWE-309).

6.3.1.12 Path Vulnerability (CWE-21)

Description

"This category [Path Vulnerability]," states OWASP, "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." [§6.6-1]

Examples

- Path traversal attack (CWE-22),
- Relative path traversal attack (CWE-23),
- Virtual files attack (CWE-66),
- Path equivalence attack (CWE-41), and
- Link following attack (CWE-59).

6.3.1.13 Protocol Errors (CWE-254, CWE-573, CWE-668)

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 (CWE-353),
- Failure to check for certificate revocation (CWE-299),
- Failure to check integrity check value (CWE-354),
- Failure to encrypt data (CWE-311),
- Failure to follow chain of trust in certificate validation (CWE-296),
- Failure to protect stored data from modification (CWE-766, CWE-767),
- Failure to validate certificate expiration (CWE-298),
- Failure to validate host-specific certificate data (CWE-297),
- Key exchange without entity authentication (CWE-322),
- Storing passwords in a recoverable format (CWE-257),
- Trusting self-reported domain name service (DNS) name (CWE-292),
- Trusting self-reported IP address (CWE-291),
- Use of hard-coded password (CWE-798, CWE-259),
- Insufficient transport layer protection (CWE-818),
- Use of weak secure socked layer / transport layer security (SSL/TLS) protocols (CWE-757),
- SSL/TLS key exchange without authentication (CWE-322),
- SSL/TLS weak key exchange (CWE-326), and
- Low SSL/TLS cipher strength (CWE-326).

Potential Impact

Compromise of security protocols such as TLS.

6.3.1.14 Range and Type Error Vulnerability (CWE-118, CWE-136)

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 (CWE-602, CWE-425),
- Buffer overflow (CWE-120),
- Buffer underwrite (CWE-124),
- Comparing classes by name (CWE-486),
- De-serialization of untrusted data (CWE-502),
- Doubly freeing memory (CWE-415),
- Failure to account for default case in switch (CWE-478),
- Format string (CWE-134),
- Heap overflow (CWE-122),
- Illegal pointer value (CWE-466),
- Improper string length checking (CWE-135),
- Integer coercion error (CWE-192),
- Integer overflow (CWE-190, CWE-680),
- Invoking untrusted mobile code (CWE-494),
- Log forging (CWE-117),
- Log injection (CWE-117),
- Miscalculated null termination (CWE-170),
- Null dereference (CWE-476, CWE-690),
- Often misused: string management (CWE-251),
- Reflection injection (CWE-470),
- Sign extension error (CWE-194),
- Signed to unsigned conversion error (CWE-195),
- Stack overflow (CWE-121),
- Truncation error (CWE-197),
- Trust boundary violation (CWE-501),
- Unchecked array indexing (CWE-129),
- Unsigned to signed conversion error (CWE-196),
- Using freed memory (CWE-416),
- Validation performed in client (CWE-602), and
- Wrap-around error (CWE-128).

6.3.1.15 Sensitive Data Protection Vulnerability (CWE-199)

Description

OWASP describes the sensitive data protection vulnerability as follows:

> 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 life cycles, 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. [§6.6-1]

Examples

- Information leakage results from insufficient memory clean-up (CWE-226),
- Inappropriate protection of cryptographic keys[2] (CWE-311, CWE-326, CWE-321, CWE-325, CWE-656),
- Lack of integrity protection for stored user data (CWE-693),
- Hard-coded password (CWE-259),
- Heap inspection (CWE-244),
- Information leakage (CWE-200),
- Password management: hardcoded password (CWE-259),
- Password plaintext storage (CWE-256), and
- Privacy violation (CWE-359).

6.3.1.16 Session Management Vulnerability (CWE-718)

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,

[2] http://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage

- 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 (CWE-6),
- Session Fixation (CWE-384),
- Cross site request forgery (CWE-352),
- Cookie attributes not set securely (e.g. domain, secure and HTTP only) (CWE-614), and
- Overly long session timeout (CWE-613).

6.3.1.17 Concurrency, Synchronization and Timing Vulnerability (CWE-361)

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 (CWE-294),
- Covert timing channel (CWE-385),
- Failure to drop privileges when reasonable (CWE-271, CWE-653),
- Failure to follow guideline/specification (CWE-573),
- File access race condition: TOCTOU (CWE-367),
- Member field race condition (CWE-488),
- Mutable object returned (CWE-375),
- Overflow of static internal buffer (CWE-500),
- Race conditions (CWE-362),
- Reflection attack in an auth protocol (CWE-301),
- State synchronization error (CWE-373), and
- Unsafe function call from a signal handler (CWE-479).

6.3.1.18 Insufficient Safeguards for Mobile Code (CWE-490)

Description

Mobile code consists of programming instructions transferred from server to client that execute on the client machine without the user explicitly initiating that execution. Allowing mobile code

generally increases attack surface. This subsection includes issues that permit the execution of unsafe mobile code.

Examples

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

6.3.1.19 Buffer Overflow (CWE-119, CWE120)

Description

Software used to implement an industrial control system (ICS) could be vulnerable to buffer overflows; adversaries could exploit these to perform various attacks. [§6.6-3]

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. [§6.6-4]

Examples [§6.6-4]

- 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 "<", and
- CVE-2003-0595 – By replacing a valid cookie value with an extremely long string of characters, an attacker may overflow the application's buffers.

6.3.1.20 Mishandling of Undefined, Poorly Defined, or “Illegal” Conditions (CWE-388, CWE-20)

Description

Some ICS implementations are vulnerable to packets that are malformed or contain illegal or otherwise unexpected field values [§6.6-3]

6.3.1.21 Use of Insecure Protocols (CWE-720)

Description

Protocols are expected patterns of behavior that allow communication 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, [§6.6-3]
- Use of clear text protocols such as FTP and Telnet
- Use of proprietary protocols lacking security features

6.3.1.22 Weaknesses that Affect Files and Directories CWE-632)

Description

Weaknesses in this category affect file or directory resources [§6.6-4]

Examples

- UNIX path link problems (CWE-60),
- Windows path link problems (CWE-63),
- Windows virtual file problems (CWE-68),
- Mac virtual file problems (CWE-70),
- Failure to resolve case sensitivity (CWE-178),
- Path traversal (CWE-22),
- Failure to change working directory in chroot jail (CWE-243),
- Often misused: path manipulation (CWE-785),
- Password in configuration file (CWE-260),
- Improper ownership management (CWE-282),
- Improper resolution of path equivalence (CWE-41),
- Information leak through server log files (CWE-533),
- Files or directories accessible to external parties (CWE-552),
- Improper link resolution before file access ('link following') (CWE-59),
- Improper handling of windows device names (CWE-67), and
- Improper sanitization of directives in statically saved code ('static code injection') (CWE-96).

6.3.1.23 4.2.1. API Abuse (CWE-227)

Description

OWASP describes the API abuse vulnerability as follows:

> 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.

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. [§6.6-1]

Examples

- Dangerous function (CWE-242, CWE-676),
- Directory restriction error (CWE-243),
- Failure to follow guideline/specification (CWE-573),
- Heap inspection (CWE-244),
- Ignored function return value (CWE-252),
- Object model violation: just one of equals() and hashCode() defined (CWE-581),
- Often misused: authentication (CWE-247),
- Often misused: exception handling (CWE-248),
- Often misused: file system (CWE-785),
- Often misused: privilege management (CWE-250), and
- Often misused: string management (CWE-251).

6.3.1.24 Use of Dangerous API (CWE-242, CWE-676)

Description

A dangerous API is one that is not guaranteed to work safely in all conditions or can be used safely but could introduce a vulnerability if used in an incorrect manner.

Examples

- Dangerous function such as the C function gets() (CWE-242),
- Directory restriction error (CWE-243),
- Failure to follow guideline/specification (CWE-573),
- Heap inspection (CWE-244),
- Insecure temporary file (CWE-377),
- Object model violation: just one of equals() and hashCode() defined (CWE-581),
- Often misused: exception handling (CWE-248),
- Often misused: file system (CWE-785),
- Often misused: privilege management (CWE-250),
- Often misused: string management (CWE-251),

- Unsafe function call from a signal handler (CWE-479), and
- Use of obsolete methods (CWE-477).

6.4 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.

6.4.1 Design

6.4.1.1 Use of Inadequate Security Architectures and Designs

Description

Development schedule pressures and lack of security training can lead to the use of inadequate security architectures and designs. This includes reliance on in-house security solutions, security through obscurity, and other insecure design practices.

Examples

- Security design by untrained engineers,
- Reliance on nonstandard techniques and unproven algorithms, and
- Security through obscurity.

6.4.1.2 Lack of External or Peer Review for Security Design

Description

Lack of understanding regarding the complexity of secure systems leads designers to believe that proven techniques can be easily combined into a larger system while preserving the security of the individual techniques. These kinds of errors are often discovered only through thorough, external review.

Examples:

- Introduction of side-channel attacks;
- Poorly combined algorithms;
- Lack of understanding regarding identifying weakest links; and
- Insufficient analysis of cascaded risk, whereby compromise of one system leads to compromise of a downstream system.

6.4.2 Implementation

6.4.2.1 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. [§6.6-3]

Examples

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

6.4.2.2 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 pre-Vista Microsoft operating systems) 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.

6.4.2.3 Absent or Deficient Equipment Implementation Guidelines

Description

Unclear implementation guidelines can lead to unexpected behavior.

A system needs 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 intended for internal use may be more vulnerable than an interface designed 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.

6.4.3 Operational

6.4.3.1 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 either 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.

6.4.3.2 Unneeded Services Running

Description

Many operating systems 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 run only if needed, and an unneeded service is a vulnerability with no benefit.

6.4.3.3 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 a remote power disconnect command is issued to *x* number of meters within a certain time, alerts should also be sent.

Examples

- Inadequate network security architecture [§6.6-3, Table 3-8];
- Inadequate firewall and router logs [§6.6-3, Table 3-11];
- No security monitoring on the network [§6.6-3, Table 3-11]; and
- Critical monitoring and control paths are not identified [§6.6-3, Table 3-12].

Potential Impact

- Failure to detect critical events;
- Removal of forensic evidence; and
- Log wipes.

6.4.4 Poorly configured security equipment (800-82 3-8)

6.4.4.1 Inadequate Anomaly Tracking

Description

Alerts and logging are two useful techniques for detecting and mitigating the risk of anomalous events but can present security risks or become vulnerabilities if not instituted thoughtfully. The appropriate reaction to an event will vary according to the criticality of the event or a correlation of certain events. The event may also need to be logged, and a central logging facility may be necessary for correlating events. Appropriate event reactions could include automatic paging of relevant personnel in the event of persistent tamper messages or may require positive

acknowledgement to indicate supervisory approval has been attained before executing a potentially disruptive command (e.g., simultaneously disconnecting many loads from the electrical grid or granting control access rights to hundreds of users).

6.5 NETWORK

Networks are defined by connections between multiple locations or organizational units and are composed 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 do not conform to required standards and compliance polices as they relate to the data exchanged.

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

6.5.1 Network

6.5.1.1 Inadequate Integrity Checking

Description

The integrity of message protocol and message data should be verified before routing or processing. Devices receiving data not conforming 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 the data were correctly received.

Such verification 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 perform logical bounds checking, such as preventing the shutdown of all power across an entire neighborhood area network (NAN).

Most functions of the Smart Grid, such as demand response (DR), load shedding, automatic meter reading (AMR), time of use (TOU), and distribution automation (DA), require that data confidentiality and/or data integrity be maintained to ensure grid reliability, prevent fraud, and enable 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 [§6.6-3, Table 3-12];
- Failure to detect and block malicious traffic in valid communication channels;
- Inadequate network security architecture [§6.6-3, Table 3-8];
- Poorly configured security equipment [§6.6-3, Table 3-8]; and
- No security monitoring on the network [§6.6-3, Table 3-11].

Potential Impact

- Compromise of smart device, head node, or utility management servers,

- Buffer overflows,
- Covert channels,
- Man-in-the-middle (MitM), and
- Denial of service or distributed denial of service (DoS /DDoS).

6.5.1.2 Inadequate Network Segregation

Description

Network architectures often do a poor job of defining security zones and controlling traffic between security zones, thus providing what is considered a flat network wherein traffic from any portion of the network is allowed to communicate with any other portion of the network. Smart Grid examples of inadequate network segregation might include 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 [§6.6-3, Table 3-10];
- Improperly configured VLAN;
- Inadequate access controls applied [§6.6-3, Table 3-8];
- Inadequate network security architecture [§6.6-3, Table 3-8];
- Poorly configured security equipment [§6.6-3, Table 3-8];
- Control networks used for non-control traffic [§6.6-3, Table 3-10];
- Control network services not within the control network [§6.6-3, Table 3-10]; and
- Critical monitoring and control paths are not identified [§6.6-3, Table 3-12].

Potential Impact

- Direct compromise of any portion of the network from any other portion of the 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; and
- Unauthorized multi-homing.

6.5.1.3 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 MitM 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 [§6.6-3, Table 3-12]; and
- Inadequate data protection is permitted between clients and access points [§6.6-3, Table 3-13].

Potential Impact

- Compromise of all authentication and payload data being passed;
- Session Hijacking;
- Authentication Sniffing;
- MitM Attacks; and
- Session Injection.

6.5.1.4 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 [§6.6-3, Table 3-12];
- Insecure key storage;

- Insecure key exchange;
- Insufficient account lockout;
- Inadequate authentication between clients and access points [§6.6-3, Table 3-13]; and
- Inadequate data protection between clients and access points [§6.6-3, Table 3-13].

Potential Impact

- DoS / DDoS;
- MitM;
- Session Hijacking;
- Authentication Sniffing; and
- Session Injection.

6.5.1.5 Insufficient Redundancy

Description

Architecture does not provide for sufficient redundancy, thus exposing the system to intentional or unintentional denial of service.

Examples

- Lack of redundancy for critical networks [§6.6-3, Table 3-9].

Potential Impact

- DoS / DDoS.

6.5.1.6 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 [§6.6-3, Table 3-9];
- Loss of environmental control [§6.6-3, Table 3-9]; and

- Noncritical personnel have access to equipment and network connections [§6.6-3, Table 3-9].

Potential Impact

- Malicious configurations;
- MitM;
- EEPROM dumping;
- Micro controller dumping;
- Bus snooping; and
- Key extraction.

6.6 REFERENCES

The following are cited in this chapter—

1. Open Web Application Security Project, April 2010, http://www.owasp.org/index.php/Category:Vulnerability
2. NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
3. NIST SP 800-82, DRAFT *Guide to Industrial Control Systems Security*, September 2008, http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf
4. CWE – Common Weakness Enumeration, http://cwe.mitre.org
5. CVE – Common Vulnerabilities and Exposures, http://cve.mitre.org/
6. NERC Critical Infrastructure Protection Standards, http://www.nerc.com/
7. NIST SP 800-27 Rev. A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
8. *CMMI® for Development, Version 1.2*, http://www.sei.cmu.edu/downloads/cmmi/CMMI-DEV-v1.2.doc
9. ISO/IEC 21827:2008, Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®), http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44716
10. Open Web Application Security Project, " Testing for business logic (OWASP-BL-001)",August 2010, http://www.owasp.org/index.php/Testing_for_business_logic_%28OWASP-BL-001%29

CHAPTER SEVEN
BOTTOM-UP SECURITY ANALYSIS OF THE SMART GRID

7.1 SCOPE

A subgroup of the 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 is to perform the analysis from the 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 is intended to complement the top-down efforts being followed elsewhere in the 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 CSWG, and to provide an independent completeness check for top-down gap analyses. This effort is proceeding simultaneously in several phases.

First, we have identified a number of *evident and specific security problems* in the Smart Grid that are amenable to and should have open and interoperable solutions but which 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 have continued to add to this list of problems as we came 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 enumerated 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 that 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.

7.2 EVIDENT AND SPECIFIC CYBER SECURITY PROBLEMS

This subsection documents specific cyber security problems in the Smart Grid insofar 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.

7.2.1 Authenticating and Authorizing Users to Substation IEDs

The problem addressed in this subsection 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 that 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 performing the role in question, possibly including nonutility 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 are seldom changed.

A 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, a wired network connection, or possibly via a wireless connection. The device may also be accessed remotely over a low-speed (dial-up) 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 Remote Authentication Dial In User Service (RADIUS) or Lightweight Directory Access Protocol (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.

7.2.2 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 that 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 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.

7.2.3 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 individual 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 that 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 advanced metering infrastructure (AMI) infrastructure.

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.

7.2.4 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.

7.2.5 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.

7.2.6 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 in 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 preprovisioned 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 DR signals. It should not be possible for a broad denial of service (DoS) attack to cause a large number of HAN devices to fail to authenticate and thereby not respond to a DR event.

7.2.7 Authenticating Meters to/from AMI Networks

Meters and AMI networks are more susceptible to widespread compromise and DoS attacks if no authentication and access control is provided in AMI access networks such as neighborhood area networks (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 that 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 for non-mesh networks due to the difference in trust models between mesh and non-mesh networks. One trust model for mesh networks is based on a 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 coexist in the same mesh network. When two or more interconnected 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 pre-distribution schemes [§7.5-11] that are resistant to node capture and operate well on devices with limited computational capabilities.

7.2.8 Securing Serial SCADA Communications

Many substations and distribution communication systems still employ slow serial links for various purposes, including supervisory control and data acquisition (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 cleartext form. Solutions that simply wrap a serial link message into protocols like Secure Socket Layer (SSL) or Internet Protocol Security (IPSec) over Point-to-Point Protocol (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.

7.2.9 Securing Engineering Dial-up Access

Dial-up 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.

7.2.10 Secure End-to-End Meter to Head End Communication

Secure end-to-end communications protocols such as transport layer security (TLS) and IPSec 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 DR control services.

7.2.11 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 (SEM) paradigm to be developed, 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 by attackers that might have subtle misconfigurations 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 the power grid infrastructure.

7.2.12 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 the correct version of untampered firmware with appropriate settings and has *always* been running untampered firmware. Remote attestation is particularly important for meters given the easy physical accessibility of meters to attackers.

7.2.13 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 connectivity 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 the IEEE 802.11i and 802.11w security standards 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, because it is outside of the scope of routing protocols. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without end-to-end security (like IPsec), attacks such as eavesdropping, impersonation, and man-in-the-middle (MITM) could be easily mounted on AMI traffic. With end-to-end security in place, routing security is still required to prevent denial of service (DoS) attacks.

7.2.14 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 tie up a line and effectively become a denial of service attack. 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.

7.2.15 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 wide area network (WAN) link will be over a relatively low bandwidth medium such as cellular band wireless (e.g., Evolution Data Optimized (EvDO), General Packet Radio Service (GPRS)), or radio networks like FlexNet. The link layer security supported by these networks varies greatly. Later versions of WiMax can utilize Extensible Authentication Protocol (EAP) for authentication, but NIST Special Publication (SP) 800-127, *DRAFT Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies,* 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 virtual private network (VPN) connection. Given the proliferation of botnets, it is not farfetched to imagine enough wireless users being compromised to launch a DoS attack 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 were rendered mostly unusable to first responders. Similar congestion events could disrupt utility communications relying on commercial WAN links.

7.2.16 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 ensure 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 ensure 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 or group of meters in a peer-to-peer mesh environment and isolate and contain any subsequent attempts to penetrate other devices. This is important, as it must be assumed that if an attacker has the capability to reverse engineer a device that any inbuilt protections can eventually be compromised as well. It is an open and challenging problem to do intrusion detection in a peer-to-peer mesh environment.

7.2.17 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 analyzing various types of electromagnetic radiation emitted by a central processing unit (CPU), display, keyboard, etc. Van Eck phreaking in particular can reconstruct the contents of a screen from the radiation emitted by the cathode ray tube (CRT) or liquid crystal display (LCD), and can be performed at some distance. TEMPEST attacks are nearly impossible to detect. Syringe attacks use a needle syringe 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. In any side-channel attack, it is not necessary for an attacker to determine the entire key; the attacker needs only enough of the key to facilitate the 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.

7.2.18 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.

7.2.19 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 Control Systems Security Working Group (CSSWG) document, *Security Guideline for the Electricity Sector: Time Stamping 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." [§7.5-14] Some detailed examples follow.

7.2.19.1 Security Protocols

Time has impact on multiple security protocols, especially in regard to the integrity of authentication schemes and other operations, if it is invalid or tampered with. For example, some protocols can rely on time stamp information to ensure against replay attacks or in other cases against time-based revoked access. Due care needs to be taken to ensure that time cannot be tampered with in any system or if it is, to ensure that the breach can be detected, responded to, and contained.

7.2.19.2 Synchrophasors

Syncrophasor measurement units are increasingly 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.

7.2.19.3 Certificates Time & Date Issues

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 could be rejected as expired. This could result in incorrect authentication or rejection of users, incorrect establishment or rejection of VPN tunnels, etc. The Kerberos network authentication protocol (on which Windows domain authentication is based) also depends critically on synchronized clocks.

7.2.19.4 Event Logs and Forensics

Time stamps 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 an 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.

7.2.20 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 that 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 a 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, thus giving rise to an unintended financial motivation to bypass security or safety measures.

7.2.21 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 in that 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, reroute traffic from the proper destination to the attacker, and perform MITM attacks on protocols that are normally limited to the inside of the substation.

7.2.22 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 among all devices.

7.2.23 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.

7.2.24 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 Distributed Network Protocol (DNP) over Transmission Control Protocol (TCP). IEC 62351 (which is the security standard 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.

7.2.25 License Enforcement Functions

Vendors and licensors are known to have embedded functions in devices and applications to enforce terms and conditions of licenses and other contracts. When exercised either intentionally or inadvertently, these functions can affect a DoS or even destroy data on critical systems. These functions occur in four general categories:

- **Misuse of authorized maintenance access.** The classic case involves a major consumer product warehouse system where there is a software dispute and the vendor disables the system through a previously authorized maintenance port.

- **Embedded shutdown functions.** Some applications contain shutdown functions that operate on a predetermined schedule unless the user performs a procedure using information supplied by the vendor. The necessary information is supplied to the user if the vendor believes the terms and conditions are being met. If the functions contain errors, they can shut down prematurely and cause DoS. This has reportedly happened on at least one mission-critical hospital-related system.
- **Embedded capability for the licensor to intrude and shut down the system.** Authority for such intrusions is contained in the Uniform Computer Information Transactions Act (UCITA).[3] This uniform state law was promulgated by the Conference of Commissioners on Uniform State Laws, and was highly controversial. It was enacted in Maryland and Virginia, but several states enacted "bomb-shelter" legislation preventing its applicability to consumers and businesses in their states. The intrusion authority is termed "self-help," which is the term used in commercial law for repossession of automobiles and other products by lenders where the purchaser has defaulted. For the licensor to be able to intrude if they believe there is noncompliance with license terms, it is necessary for the operating system or application to have an embedded backdoor.
- **Requiring the application or device to contact a vendor system over the public Internet.** This may occur to authorize initial startup or regularly during operation. It is problematic if the application or device has security requirements that prevent access to the public Internet.

7.2.26 Unmanaged Call Home Functions

Many recent commercial off-the-shelf (COTS) software applications and devices attempt to connect to public IP addresses in order to update software or firmware, synchronize time, provide help/support/diagnostic information, enforce licenses, or utilize Internet resources such as mapping tools, search systems, etc. In many cases, use of such call home functions is not obvious and is poorly documented, if any documentation exists. Configuration options to modify or disable call home functions are often hard to find if available. Examples of such call home functions include:

- Operating system updaters;
- Application updaters, including Web browsers, rendering tools for file formats such as PDF, Flash, QuickTime, Real, etc., printing software and drivers, digital camera software, etc.;
- Network devices that obtain time from one or more Network Time Protocol (NTP) servers;
- Voice-over-Internet-Protocol (VoIP) devices that register with a public call manager;
- Printers that check for updates and/or check a Web database to ensure valid ink cartridges;
- Applications that link to Web sites for documentation; and

[3] http://www.ucitaonline.com/

- Applications that display information using mapping tools or Google Earth.

Some call home functions run only when an associated application is used; some are installed as operating system services running on a scheduled basis; and some run continuously on the device or system. Some call home updaters request confirmation from the user before installing updates, while others quietly install updates without interaction. Some call home functions use insecure channels.

Unexpected call home functions that are either unknown to or not anticipated by the Smart Grid system designer can have serious security consequences. These include:

- Network information leakage;
- Unexpected changes in system configuration through software, firmware, or settings updates;
- Risk of network compromise via compromise of the call home channel or external endpoint;
- Unexpected dependence on external systems, including not only the systems that the call home function calls, but also public DNS and public time sources;
- False positives on IDS systems when outbound connection attempts from call home functions are blocked by a firewall;
- System resource consumption; and
- Additional resource consumption when call home functions continuously attempt to retry connections that are blocked by a firewall.

For the specific case of software or firmware updaters, best practices for patch management recommend deploying patch servers that provide patches to endpoints rather than having those endpoints reach out to the Internet. This provides better control of the patching process. However, most applications use custom updating mechanisms, which can make it difficult to deploy a comprehensive patch system for all operating systems, applications, and devices that may be used by the Smart Grid system. Further, not all applications and devices provide a way to change their configuration to direct them to a patch server.

7.3 NONSPECIFIC CYBER SECURITY ISSUES

This subsection lists cyber security issues that are too abstract to describe in terms of specific security problems but when considered in different contexts (control center, substation, meter, HAN device, etc.) are likely to lead to specific problems.

7.3.1 IT vs. Smart Grid Security

The differences between information technology (IT), industrial, and Smart Grid security need to be accentuated in any standard, guide, or roadmap document. NIST SP 800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*, can be used as a basis, but more needs to be addressed in that control system security operates in an industrial campus setting and is not the same as an environment that has the scale, complexity, and distributed nature of the Smart Grid.

7.3.2 Patch Management

Specific devices such as IEDs, PLCs, smart meters, etc., will be deployed in a variety of environments and critical systems, and their accessibility may necessitate undertaking complex activities to enable software upgrades or patches because of how distributed and isolated the equipment can be. Also, many unforeseen consequences 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 life cycle 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 need 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 whereby the risk and impact of vulnerability can be determined in order to prioritize upgrades. A security infrastructure also needs to be in place that can mitigate possible threats until needed upgrades can be qualified and deployed so that the reliability of the system can be maintained.

7.3.3 Authentication

There is no centralized authentication in the decentralized environment of the power grid, and authentication systems need to be able to operate in this massively distributed and locally autonomous setting. For example, substation equipment such as IEDs needs to have access controls that allow only authorized users to configure or operate them. However, credential management schemes for such systems cannot rest on the assumption that a constant network connection to a central office exists to facilitate authentication processes. What is called for are secure authentication methods that allow for local autonomy when needed and yet can provide for revocation and attribution from a central authority as required. Equally important is the recognition that any authentication processes must securely support emergency operations and not become an impediment at a critical time.

7.3.4 System Trust Model

There has to be a clear idea of what elements of the system are trusted—and to what level and why. Practically speaking, there will always be something in the system that has to be trusted; the key is to 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 the former poses less risk. However, even here there are dependencies based on the design and management of that network that would inform the trust being vested in it.

7.3.5 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." TPI is a security measure to prevent single-person access to key management mechanisms. This practice comes from national security environments but may have some applicability to the Smart Grid where TPI security measures might be thought of as somewhat similar to the safety precaution of 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).

7.3.6 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.

7.3.7 Distributed vs. Centralized Model of Management

There are unique issues respecting how to manage something as distributed as the Smart Grid and yet maintain good efficiency and reliability factors that imply centralization. Many grid systems are highly distributed, are 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 the "hybrid" approach necessary for the Smart Grid.

7.3.8 Local Autonomy of Operation

Any security system must have local autonomy; for example, it cannot always be assumed there is 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 from being taken.

7.3.9 Intrusion Detection for Power Equipment

One issue specific to power systems is handling specialized protocols like Modbus, DNP3, 61850, etc., and standardized IDS and security event detection and management models need to be built for these protocols and systems. More specifically, these models need to represent a deep contextual understanding of device operation and state to be able to detect when anomalous commands might create an unforeseen and undesirable impact.

7.3.10 Network and System Monitoring and Management for Power Equipment

Power equipment does not necessarily use common and open monitoring protocols and management systems. Rather, those systems often represent 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 the Simple Network Management Protocol (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.

7.3.11 Security Event Management

Building on more advanced IDS forms 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 need to be clear methods of incident response to events that are 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.

7.3.12 Cross-Utility / Cross-Corporate Security

Unfortunately, many Smart Grid deployments are going forward without much thought to what happens behind the head end AMI systems and further on down the line for SCADA and other real-time control systems supporting 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 DR control centers will handle integration with head end systems. Moreover, in many markets, the company that controls the head end to the 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 system, 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 either accidentally or maliciously.

7.3.13 Trust Management

Appropriate trust of a device must be based on the physical and logical ability to protect that device, and on protections available in the network. There are many devices that are physically accessible to adversaries by the nature of their locations, such as meters and pole-top devices, which also have limited anti-tamper protections due to cost. Systems that communicate with these devices should use multiple methods to validate messages received, should be designed to account for the possibility that exposed devices may be compromised in ways that escape detection, and should never fully trust those devices.

For example, even when communicating with meters authenticated by public key methods and with strong tamper resistance, unexpected or unusual message types, message lengths, message content, or communication frequency or behavior could indicate that the meter's tamper resistance has been defeated and its private keys have been compromised. Such a successful attack on a meter must not result in possible compromise of the AMI 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 the criticality of the system (i.e., most decisions are based on how important the system is). In this type of trust management, each system in the Smart Grid is categorized not only for its own needs (CI&A, etc.) but according to the required trust and/or limitations on trust mandated by our ability to control physical and logical access to it and the 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.

7.3.14 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.

7.3.15 Password Management

Passwords for authentication and authorization present many problems when used with highly distributed, decentralized, and variedly connected systems such as the Smart Grid. Unlike enterprise environments where an employee typically accesses organization services from one, or at most a few, desktop, laptop, or mobile computing systems, maintenance personnel may need to access hundreds of different devices, including IEDs, RTUs, relays, meters, etc. These devices may sometimes be accessed remotely from a central site, such as a control center, using simple tools such as terminal emulators, sometimes from a front panel with keyboard, sometimes from a locally connected laptop using a terminal emulator, or sometimes from specialized local access ports such as the optical port on a meter. Access must be able to operate without relying on communications to a central server (e.g., RADIUS, Active Directory) since access may be required for power restoration when communications are out. Setting different passwords for every device and every user may be impractical—see Sections 7.2.1, 7.2.2, 7.2.3, and 7.2.9.

NIST SP 800-118, *DRAFT Guide to Enterprise Password Management*, gives reasonable guidance regarding password complexity requirements, but the password management techniques it describes will often be inapplicable due to the nature of power system equipment as discussed above. Suitable password management schemes need to be developed—if possible—that take into account both the nature of Smart Grid systems and of users. Alternatively, multi-factor authentication approaches should be considered.

7.3.16 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.

7.3.17 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 Web site address. In Web systems, this problem is solved by SSL certificates that include the Domain Name Service (DNS) identity.

7.3.18 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.

7.3.19 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.

7.3.20 Legacy Equipment with Limited Resources

The life cycle of equipment in the electricity sector typically extends beyond 20 years. Compared to IT systems, which typically see 3–5 year life cycles, 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 would be 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.

7.3.21 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 cost versus benefit of the security measure in the risk mitigation and decision process can prove prohibitive for the deployment if the cost outweighs the benefits of the deployed 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 the lack of centralized and remote patch/firmware management solutions, contributes 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. Extensive regression testing is extremely important to ensure that an upgrade to a device will not negatively impact reliability, but that testing 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.

7.3.22 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 concerns, little 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 the 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 necessitates 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 to gather evidentiary material where applicable and that the tools be provided to maintain chain of custody, reduce the risk of spoliation, and ensure that the origin of the evidence can be properly authenticated. Tools should be capable of retrieving data from meters, collectors, and 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.

7.3.23 Roles and Role-Based Access Control

A *role* is a collection of permissions that may be granted to a user. An individual 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, nontechnical levels of the GridWise Architecture Council [GWAC] stack).

Issues in implementing role-based access control (RBAC) include the following:

1. The extent to which roles should be predefined 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; and
- 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 nonhierarchical 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 cannot 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?

7.3.24 Limited Sharing of Vulnerability and/or Incident Information

There is a significant reticence with respect to sharing information about vulnerabilities or incidents in any critical infrastructure industry. This is based on many sound reasons—not the least of which may be 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 third party, be it government or private institution.

7.3.25 Data Flow Control Vulnerability Issue

The power grid will encompass many networks and subnetworks, 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 a 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.

7.3.26 Public vs. Private Network Use

There is ongoing debate in the industry over the use of public network infrastructures such as the Internet or of the public cellular or WiMax networks that telecommunication companies provide. (Here the term *public network* should not be confused with the use of the Internet Protocol or 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), such a scheme carries significantly more risk of intrusion, disruption, tampering, and general reliability regardless of the countermeasures in place. This is true because of 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 should be self-evident facts 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, are 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); and
- Identifying countermeasure systems (e.g., firewalls, IDS/IPS, SEM, encrypted links and 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.

7.3.27 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; and
- 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 Federal Energy Regulatory Commission (FERC) Order No. 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.

7.3.28 Poor Software Engineering Practices

Poor software engineering practices, such as those identified in NISTIR 7628, Chapter 7, "Vulnerability Classes," 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 [§7.5-12], 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.

7.3.29 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.

7.3.30 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 upon. 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.

7.3.31 Broad Definition of Availability

One of the stated goals of the NIST cyber security effort is to assure "availability" at the application level. "Availability" according to the DHS *Catalog of Control Systems Security: Recommendations for Standards Developers* [§7.5-13], is—

> Availability— The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

Presenting such a broad definition to the power delivery organization responsible for achieving that availability, considering the complexity of the Smart Grid, represents a very substantial and perhaps impractical challenge, for several reasons—

- The system, being so broadly defined, could be considered many different systems or many different combinations of systems. Does the system need to be defined as including all of the Smart Grid applications? Does it include future applications?

- As a result, just defining what the "system" is that is being protected could be difficult to reach consensus on.
- "Performance specifications" even for well-defined systems such as a SCADA system will often not be stated in a way that allows underlying media and subsystems to be evaluated. For example, most SCADA systems are designed with certain maximum poll rates and response times, but not necessarily with any requirement for availability in terms of communication interruptions or interference effects. These systems are usually purchased in pieces, with master stations, communications, and field equipment as entirely separate components without any overall specification of the system performance requirements. Thus, the traceability of the performance of all of the individual components and features to system availability as a whole may prove to be extremely difficult.
- Availability in power system reliability means something different from availability (or non-denial of service) in security.
- "Usable upon demand" in the definition of availability could mean many things in terms of response time.

If these systems were used for different purposes, perhaps some very general, functional requirements would suffice to guide the use of the Roadmap by the power delivery organizations. However, all of these systems deliver power; they are all structured similarly, with generation, transmission, and distribution as separate but interconnected systems.

7.3.32 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, with each calling out different requirements. This can have an adverse affect on both interoperability and security.

7.3.33 Cyber Security Governance

From the IT Governance Institute (ITGI), and adopted by the Chartered Institute of Management Accountants (CIMA) and the International Federation of Accountants (IFAC), *governance* is defined as follows:

> 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 for the Smart Grid is strategic direction: ensuring that goals and objectives are achieved, that business risk (including security risk) is managed appropriately, that resource utilization is efficiently and effectively managed in a responsible fashion, and that enterprise security activities are monitored to ensure success or risk mitigation as needed if there are failures in security.

Since cyber security (information security), as opposed to IT security, encompasses an overall perspective on all aspects of data/information (whether spoken, written, printed, electronic, etc.) and how it is handled—from its creation to how it is viewed, 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 its executive management must be cognizant of the risks that must be taken into account regarding what vulnerabilities to security threats of any sort may ensue if Smart Grid systems are not created and managed carefully and how such risks may be mitigated.[4]

Borrowing again from ITGI and its guide to "Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition," the following represents 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.

[4] See Title XIII, Section 1309 of the Energy Independence and Security Act of 2007 (EISA), U.S Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE).

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.

7.4 DESIGN CONSIDERATIONS

This subsection discusses cyber security 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.

7.4.1 Break Glass Authentication

Authentication failure must not interfere with the need for personnel to perform critical tasks during an emergency situation. An alternate form of "break glass" authentication may be necessary to ensure that access can be gained to critical devices and systems by personnel when ordinary authentication fails for any reason. A "break glass" authentication mechanism should have the following properties—

- Locally autonomous operation—to prevent failure of the "break glass" authentication mechanism due to failure of communications lines or secondary systems;
- Logging—to ensure that historical records of use of the "break glass" mechanism, including time, date, location, name, employee number, etc., are kept;
- Alarming—to report use of the "break glass" mechanism in real-time or near real-time to an appropriate management authority, e.g., to operators at a control center or security desk;
- Limited authorization—to enable only necessary emergency actions and block use of the "break glass" mechanism for non-emergency tasks; disabling logging particularly should not be allowed; and
- Appropriate policies and procedures—to ensure the "break glass" authentication is used only when absolutely necessary and does not become the normal work procedure.

Possible methods for performing "break glass" authentication include but are not limited to—

- Backup authentication via an alternate password that is not normally known or available but can be retrieved by phone call to the control center, by opening a sealed envelope carried in a service truck, etc.;
- Digital certificates stored in two-factor authentication tokens; and
- One-time passwords.

7.4.2 Biometrics

This topic will be discussed in the next version of this document.

7.4.3 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 a particular 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 SP 800-63, *Electronic Authentication Guideline*, contains some guidance on measuring password strength and recommendations for minimum password strengths.

Some considerations for password complexity rules—

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?

Draft NIST SP 800-118 gives further guidance on password complexity.

7.4.4 Authentication

There is no standard currently in the Smart Grid Framework and Roadmap that supports or provides guidance on how to accomplish strong authentication. The initial release of the NERC Critical Infrastructure Protection (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 noncritical 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 NISTIR 7628;
- NIST SP 800-63 provides a framework of requirements but is not overly prescriptive regarding implementation; and
- The multilevel 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." [§7.5-15] Multi-factor authentication is required at Levels 3 and 4. The NIST document grades the levels in terms of protection against increasingly sophisticated attacks.

7.4.5 Network Access Authentication and Access Control

Several link-layer and network-layer protocols provide network access authentication using Extensible Authentication Protocol [§7.5-1]. EAP supports a number of authentication algorithms—so called EAP methods.

Currently EAP-TLS [§7.5-2] and EAP-GPSK Generalized Pre-Shared Key) [§7.5-3] 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 [§7.5-4] provides port access control and transports EAP over Ethernet and Wi-Fi. In WiMAX, PKMv2 (Privacy Key Management version 2) in IEEE 802.16e [§7.5-5] transports EAP. PANA (Protocol for carrying Authentication for Network Access) [§7.5-6] transports EAP over UDP/IP (User Datagram Protocol/Internet Protocol). TNC (Trusted Network Connect) [§7.5-7] 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 [§7.5-8] 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, Authorization, and Accounting) protocol such as RADIUS [§7.5-9] 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 [§7.5-10] 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.

7.4.6 Use of Shared/Dedicated and Public/Private Cyber Resources

The decision whether to use the public Internet or any shared resource, public or private, will have significant impact on the architecture, design, cost, security, and other aspects of any part of the Smart Grid. This section provides a checklist of attributes with which architects and designers can conduct a cost/trade analysis of these different types of resources.

The objective of any such analysis is to understand the types of information that will be processed by the cyber resources under consideration, and to evaluate the information needs relative to security and other operational factors. These needs should be evaluated against the real costs of using different types of resources. For example, use of the public Internet may be less costly than developing, deploying, and maintaining a new infrastructure, but it may carry with it performance or security considerations to meet the requirements of the Smart Grid information that would have to be weighed against the cost savings.

Each organization should conduct its own analyses—there is not one formula that is right for all cases.

7.4.6.1 Definitions

There are two important definitions to keep in mind when performing the analysis—

1. Cyber Equipment—anything that processes or communicates Smart Grid information or commands.
2. Internet—An element of Smart Grid data is said to have used the Internet if at any point while traveling from the system that generates the data-containing message to its ultimate destination it passes through a resource with an address within an RIR (Regional Internet Registry) address space.

7.4.6.2 Checklist/Attribute Groupings

There following five lists contain attributes relevant to one dimension of the cost/trade analysis—

1. Attributes related to Smart Grid Information—this list could be viewed as the requirements of the information that is to be processed by the Smart Grid cyber resource;
    a. Sensitivity and Security Requirements;
        - Integrity,
        - Confidentiality,
        - Timeliness considerations—how long is the information sensitive?

- Availability, and
- Strategic vs. tactical information—aggregation considerations/impacts;

b. Ownership—who owns the data;

c. Who has a vested interest in the data (e.g., customer use data);

d. Performance/Capacity/Service-level requirements; and
   - Latency,
   - Frequency of transmission,
   - Volume of data,
   - Redundancy/Reliability, and
   - Quality of Service; and

e. Legal/Privacy considerations—in this context, privacy is not related to protection of the data as it moves through the Smart Grid. It is related to concerns stakeholders in the information would have in its being shared. For example, commercial entities might not wish to have divulged how much energy they use.

2. Attributes of a Smart Grid Cyber Resource—cyber resources have capabilities/attributes that must be evaluated against the requirements of the Smart Grid information;

   a. Ownership
      - Dedicated, and
      - Shared;

   b. Controlled/managed by
      - Internal management,
      - Outsourced management to another organization, and
      - Outsourced management where the resource can be shared with others;

   c. Geographic considerations—jurisdictional consideration;

   d. Physical Protections that can be used
      - Media,
        1. Wired, and
        2. Wireless.
           a. Not directed, and
           b. Directed
      - Equipment, and
      - Site;

   e. Performance/Scale Characteristics
      - Capacity per unit time (for example, a measure of bandwidth),

- Maximum utilization percentage,
- Ability to scale—are forklift upgrades needed? Related to this is the likelihood of a resource being scaled—what are the factors (economic and technical) driving or inhibiting upgrade?
- Latency, and
- Migration—ability to take advantage of new technologies;

f. Reliability;

g. Ability to have redundant elements; and

h. Known security vulnerabilities.

- Insider attacks,
- DOS,
- DDOS, and
- Dependency on other components.

3. Attributes related to Security and Security Properties—given a type of information and the type of cyber resource under consideration, a variety of security characteristics could be evaluated—including different security technologies and appropriate policies given the information processed by, and attributes of, the cyber resource.
   a. Physical security and protection;
   b. Cyber protection
      - Application level Controls,
      - Network level controls, and
      - System;
   c. Security/Access policies
      - Inter organizational, and
      - Intra organizational;
   d. Cross-administrative domain boundary policies; and
   e. Specific technologies.
4. Attributes related to Operations and Management—one of the most complex elements of a network is the ongoing operations and management necessary after it has been deployed. This set of attributes identifies key issues to consider when thinking about different types of Smart Grid cyber resources (e.g., public/private and shared/dedicated).
   a. Operations
      - People,
        1. Domain Skills (e.g., knowledge of control systems), and
        2. IT Operations Skills (e.g., systems and network knowledge).

- Processes
    1. Coordination
        a. Within a department,
        b. Across departments, and
        c. Across organizations/enterprises.
    2. Access Controls
        a. Third Party, and
            - Frequency,
            - Control, and
            - Trusted/Untrusted party (e.g., vetting process).
        b. Employees; and
    3. Auditing.

b. System-level and Automated Auditing;

c. Monitoring
    - Unit(s) monitored—granularity,
    - Frequency,
    - Alarming and events,
    - Data volume,
    - Visibility to data,
    - Sensitivity, and
    - Archival and aggregation; and

d. Management.
    - Frequency of change,
    - Granularity of change,
    - Synchronization changes,
    - Access control,
    - Rollback and other issues, and
    - Data management of the configuration information.

5. Attributes related to Costs—the cost attributes should be investigated against the different types of cyber resources under consideration. For example, while a dedicated resource has a number of positive performance attributes, there can be greater cost associated with this resource. Part of the analysis should be to determine if the benefits justify the cost. The cost dimension will cut across many other dimensions.
    a. Costs related to the data

- Cost per unit of data,
- Cost per unit of data over a specified time period, and
- Oversubscription or SLA costs;

b. Costs related to resources (cyber resources)
- Resource acquisition cost (properly apportioned),
- Resource installation cost,
- Resource configuration,
- Resource operation and management cost, and
- Monitoring cost;

c. Costs related to operational personnel
- Cost of acquisition,
- Cost of ongoing staffing, and
- Cost of Training;

d. Costs related to management software
- Infrastructure costs,
- Software acquisition costs,
- Software deployment and maintenance costs, and
- Operational cost of the software—staff, etc.; and

e. How are the common costs being allocated and shared?

7.5 REFERENCES

1. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC3748, http://www.ietf.org/rfc/rfc3748.txt, June 2004.
2. D. Simon, B. Aboba and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, http://www.ietf.org/rfc/rfc5216.txt, March 2008.
3. T. Clancy and H. Tschofenig, “Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method”, RFC5433, http://www.ietf.org/rfc/rfc5433.txt, February 2009.
4. IEEE standard for local and metropolitan area networks — port-based network access control, IEEE Std 802.1X-2004, December 2004.
5. 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.

6. D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC5191, http://www.ietf.org/rfc/rfc5191.txt, May 2008.
7. Trusted Network Connect (TNC), http://www.trustedcomputinggroup.org/developers/trusted_network_connect
8. ZigBee® Alliance, http://www.zigbee.org/
9. 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.
10. 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.
11. 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.
12. Katie Fehrenbacher "Smart Meter Worm Could Spread Like a Virus", http://earth2tech.com/2009/07/31/smart-meter-worm-could-spread-like-a-virus/.
13. Department of Homeland Security, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers*, March 2010.
14. NERC Control Systems Security Working Group (CSSWG) document, *Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs*, v. 0.995, http://www.nerc.com/docs/cip/sgwg/Timestamping_Guideline_009-11-11_Clean.pdf
15. NIST Special Publication 800-63, *Electronic Authentication Guideline*, v. 1.0.2, April 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

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

8.1 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 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 is long-term (5–10 years) and short-term (less than 5 years) 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 distills research and development themes that are meant to present paradigm changing directions in Cyber Security that will enable higher levels of reliability and security for the Smart Grid as it continues to become more technologically advanced.

The topics are based partly on the 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:

- Device Level
- Cryptography and Key Management
- Systems Level
- Networking Issues
- 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 by 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 U.S. Department of Energy Control System Security and the National SCADA Testbed programs, U.S. Department of Homeland Security Control System Security program and Cyber Physical Systems Security efforts,[5] the

[5] See https://www.enstg.com/Signup/files/DHS%20ST%20Cyber%20Workshop%20Final%20Report-v292.pdf.

industry Roadmap to Secure Control Systems, the UCA International Users group focusing on AMI security, and the North American Synchrophasor Initiative.

This document is written as an independent collection of research themes, and as such, the sections do not necessarily flow from introduction to summary.

8.2 DEVICE-LEVEL TOPICS—COST-EFFECTIVE TAMPER-RESISTANT DEVICE ARCHITECTURES

8.2.1 Improve Cost-Effective High Tamper-Resistant & Survivable Device Architectures

With intelligent electronic devices (IEDs) playing more critical roles in the Smart Grid, there is an increasing need to ensure that those IEDs 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 as to deployment and use, and the protection measures must be mass-producible. Some initial forms of these technologies are in the field, but there is a growing belief that further improvement is needed, as security researchers have already demonstrated penetrations of these devices—even with some reasonable protections in place. Further, it is important to assume devices *will be* penetrated, and there must be a method for their containment and implementing secure recovery measures using remote means. This is of great importance to maintain the reliability and overall survivability of the Smart Grid.[6]

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. Such architectures must be highly tamper-resistant and evident, and provide for secure remote recovery. Research into improved security for firmware/software upgrades is also needed. Without these R&D advances, local attacks can become distributed/cascading large-scale attack campaigns.

Potential starting points for these R&D efforts 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.

8.2.2 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 internetwork of

[6] Please see Chapter 2 for discussion of defense-in-depth on a system-wide basis that would begin to address these issues.

embedded systems. Intrusion detection in such systems does not merely consist in adapting the types of intrusion detection developed for classical IT systems.[7]

This work should 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.

8.3 CRYPTOGRAPHY AND KEY MANAGEMENT

8.3.1 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, 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 public key infrastructure (PKI), identity-based encryption (IBE), and hierarchical, decentralized, and delegated schemes and their hybridization.

There are also problems of ownership (e.g., utility vs. customer-owned) and trust, and how both can be optimally managed in environments where there is little physical protection and access may happen across different organizational and functional domains (e.g., a 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.

The various devices/systems that will be found in the areas of distributed automation, AMI, distributed generation, substations, etc., will have 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 research into more efficient, *ad hoc*, and flexible key management that requires 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 measures degrade the reliability of the system by, for example, "locking out" personnel/systems 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.

[7] Subsection 8.6.3 of this report discusses this issue in the context of protecting cyber-power systems.

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

8.3.2 Advanced Topics in Cryptography

Several security and privacy requirements for the Smart Grid may benefit from advanced cryptographic algorithms.

8.3.2.1 Privacy-enhancing cryptographic algorithms

Privacy-enhancing cryptographic algorithms can mitigate privacy concerns related to the collection of consumer data by computing functions on ciphertexts. This can be beneficial for third-party providers who want to access encrypted databases and would like to compute statistics over the data. Similarly, while utilities need to collect individual measurements for billing, they do not require real-time individual data collection to operate their network. Therefore, they can use aggregated data representing the consumption at a data aggregator. Homomorphic encryption schemes can provide computations on ciphertexts. Research is needed on extending the efficiency and generality of current homomorphic encryption schemes to provide universal computation.

8.3.2.2 Cryptographic in-network aggregation schemes

Cryptographic in-network aggregation schemes have the potential of improving the efficiency of many-to-one communications in the Smart Grid, like those generated from multiple sensors to a single or a small number of designated collection points. To achieve efficient in-network aggregation, intermediate nodes in the routing protocol need to modify data packets in transit; for this reason, standard signature and encryption schemes are not applicable, and it is a challenge to provide resilience to tampering by malicious nodes. Therefore, we require homomorphic encryption and signature schemes tailored for efficient in-network aggregation.

8.3.2.3 Identity-Based Encryption

Key distribution and key revocation are some of the most fundamental problems in key distribution for systems. IBE is a new cryptographic primitive that eliminates the need for distributing public keys (or maintaining a certificate directory) because identities are automatically bound to their public keys. This allows, for example, a third party for energy services to communicate securely to their customers without requiring them to generate their keys. IBE also eliminates the need for key revocation because IBE can implement time-dependent public keys by attaching a validity period to each public key. In addition, for enterprise systems, a key escrow is an advantage for recovering from errors or malicious insiders. IBE provides this service because the private-key generator (PKG) can obtain the secret key of participants. This property suggests that IBE schemes are suitable for applications where the PKG is unconditionally trusted. Extending this level of trust for larger federated systems is not possible; therefore, very large deployments require hybrid schemes with traditional public key cryptography and certificates for the IBE parameters of each enterprise or domain.

Alternatively, we can extend pure IBE approaches with further research on certificate-based encryption.

8.3.2.4 Access control without a mediated, trusted third party

The limited (or intermittent) connectivity of several Smart Grid devices requires further research into access control mechanisms without an online third party. Attribute-Based Encryption (ABE) is an emerging crypto-system that can be thought of as a generalization of IBE. In ABE schemes, a trusted entity distributes attribute or predicate keys to users. Data owners encrypt their data using the public parameters and attributes provided by the trusted entity or an attribute policy of their choosing. In ABE, users are able to decrypt ciphertexts only if the attributes associated with the ciphertext (or the keys of the users) satisfy the policy associated with the ciphertext (or the predicate associated with their keys); therefore, access control can be achieved without an online trusted server.

8.3.2.5 Interoperability with limited (or no) online connectivity

The limited (or intermittent) connectivity of Smart Grid devices may require local (e.g., HAN) mechanisms for key and content management. Proxy re-encryption and proxy re-signature schemes can alleviate this problem. In these schemes, a semi-trusted proxy (e.g., a HAN interoperability device) can convert a signature or a ciphertext computed under one key (e.g., the public key of device A) to another (e.g., the public key of device B), without the proxy learning any information about the plaintext message or the secret keys of the delegating party.

8.4 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 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, failover, 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 that 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 are described in the following subsections.

8.4.1 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 be achieved only

under certain conditions. To complicate things further, different applications in the 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 cover 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 while 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 needs to be escrowed or made available? How much data needs to be checkpointed and placed at what location? What is the circle of influence that needs to be considered to facilitate bounded recovery and reaction? These are the questions that the R&D task should answer.

8.4.2 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 failover for continued operation, through 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 rekeying and exploiting these strategies for grid control with security.

8.4.3 Calibrating assurance and timeliness trade-offs

There are various sources of delay in the path between two interacting entities in the Smart Grid (e.g., from the sensor that captures the measurement sample such as the PMU to the application that consumes it, or from the applications at the control center that invoke operations, upload firmware, or change parameter values to the affected remote smart device). Some such delay sources represent security mechanisms that already exist in the system, and many of these can be manipulated by a malicious adversary. To defend against potential attacks, 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 tradespace for potential solutions that are

appropriate for grid applications. Without this understanding, at times of crisis operators will be ill-prepared and will have to depend on individual intuition and expertise. On the other hand, if the trade-offs are well understood, it will be possible to develop and validate contingency plans that can be quickly invoked or offered to human operators at times of crisis.

8.4.4 Legacy system integration

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

- Compatibility problems when new security solutions are installed in new devices resulting in mismatched expectations that may cause the devices to fail or malfunction (an anecdotal story tells of a network scan using tools like the Network MAPper [NMAP] tripping IEDs because they do not fully implement the TCP/IP stack); and
- Backwards compatibility, which may often be a requirement (regulator, owner organization) and may prevent deployment of advanced features.

Relevant effort:

- Not just linking encryptors but conducting research in legacy systems beyond SCADA encryption; American Gas Association (AGA), AGA 12 Cryptography Working Group.

Potential avenues of investigation include:

- Compositionality (enhanced overlays, bump-in-the-wire[8], adapters) that contain and mask legacy systems; and
- Ensuring that the weakest link does not negate new architectures through formal analysis and validation of the architectural design, possibly using red team methodology.

8.4.5 Resiliency Management and Decision Support

Research into resiliency management and decision support 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.

8.4.6 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

[8] An implementation model that uses a hardware solution to implement IPSec.

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 upon *ad hoc* mobile radio networks.

Research that 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.

8.4.7 Risk Assessment and Management

A risk-based approach is a potential way to develop viable solutions 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 subsections describe three important ones.

8.4.7.1 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?”

8.4.7.2 Measuring Risk

The state of the art in the risk measurement 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.

8.4.7.3 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.

8.5 NETWORKING TOPICS

8.5.1 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 available Enterprise systems. Research is needed to investigate if such resources can be used in the Smart Grid reliably and safely, and how they would be implemented.

8.5.1.1 Internet Usage 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, containing numerous instances of malicious malware and malicious activities. Research into methods to deal with denial of service as well as to identify other critical issues will serve our understanding of the strengths and weaknesses as well as the cautions inherent in using the existing Internet for specific types of Smart Grid applications.

8.5.1.2 TCP/IP Security and Reliability Issues

Security/reliability issues surrounding the adoption of TCP/IP for Smart Grid networks is a related research topic separate from the subject of Internet use. Research into the adoption of Internet protocols for Smart Grid networks could include understanding the current state of security designs proposed for advanced networks. Features such as quality of service (QoS), mobility, multi-homing, broadcasting/multicasting, and other enhancements necessary for Smart Grid applications must be adequately secured and well managed if TCP/IP is to be adopted.

8.5.2 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 the National Science Foundation (NSF), Defense Advanced Research Projects Agency (DARPA), and others. Advanced networking development promises simpler approaches to networking infrastructures that solve by design some of the issues now affecting the Internet protocols. The work, although not complete, should be understood in the context of providing secure networks with fewer complexities that can be more easily managed and offer more predictable behavior.

A wide variety of communication media are currently available and being used today—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 need support these various physical layers.

8.5.3 IPv6

It is very difficult to predict the consequences of large-scale deployments of networks. As the Smart Grid will likely be based on IPv6 in the future, and it is predicted that millions of devices will be added to the Smart Grid, it is not obvious that the backbone will function flawlessly. Research is needed to ensure that the IPv6-based network will be stable, reliable, and secure.

In particular, these issues need more research—

- Will current and future protocols scale to millions of devices?
- Is current modeling, simulation, and emulation technology sufficient to model future networks using IPv6?
- How is the accuracy of projected performance validated?
- Will devices interoperate properly in multi-vendor environments?

- Are the routing protocols suitable? Do new standards need to be developed?
- Are there any security concerns? How will the network be partitioned?
- Should NAT (Network Addresses Translation) be used?
- Is a fundamentally new network architecture needed?

8.6 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, researchers, 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-energy and electric vehicles, residential customers may possibly be included. Effectively securing the interfaces between environments will become an increasing challenge as users seek to extend Smart Grid capabilities. Scalable and secure interorganizational interaction is a key security and management issue. Privacy policies involving data at rest, in transit, and in use will have to be enforced within and across these environments. Research is needed in the areas discussed in the following subsections.

8.6.1 Privacy and Access Control in Federated Systems

8.6.1.1 Managed Separation of Business Entities

Research in the area of managed separation will focus on the network and systems architecture that enables effective communication among various business entities without inadvertent sharing/leaking of their trade secrets, business strategies, or operational data and activities. It is anticipated that 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. Research into managing the separation between business entities needs to address multiple areas:

- Techniques to specify and enforce the appropriate sharing policies among entities with various cooperative, competing, and 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.
- 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.

- 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.

8.6.1.2 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), especially when the confederates enter into dynamic relationships such as daily buying/selling, long-term contracts, etc., is an issue that needs added research.

8.6.2 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 auditing and accountability a complex problem: Who is responsible for auditing whom? How are the audit trails collected at various points to be linked? What mechanism can be used to mine the data thus collected? 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 prosecuting attackers and providing evidence to regulatory agencies without interrupting operations.

8.6.3 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, 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. Research into interdependency issues would investigate and identify these dependencies and work on key concepts and plans toward mitigating the associated risks from the perspective of the Smart Grid. Such research 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 should also apply a rigorous approach to identifying and highlighting these key interdependencies across all of these critical common infrastructure elements. The research would lead to developing and applying new

system-of-systems concepts and design approaches toward mitigating the risks posed by these interdependencies on a nationwide scale.

8.6.4 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 like the Smart Grid, is not well understood. Without further research, this is going to remain a dark area that carries a big risk for the operational reliability and resiliency of the power grid.

As mentioned throughout various sections of this report, there is a need to better integrate the cyber and power system view. This is especially important in regard to detecting security events such as intrusions, unauthorized accesses, misconfigurations, 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 while not offering 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 need to further research and develop models, methods, and technologies in the following 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;
- Development of distributed IED autonomous security agents with multi-master SIEM reporting for wide area situational awareness;
- Development of distributed IED autonomous security agents with continuous event and state monitoring and archiving in the event of islanding, security state restoration and forensics when isolated from master SIEM systems;
- Advanced Smart Grid integrated security and reliability analytics that provide for event and impact prediction, and continual infrastructure resiliency improvement; and

- Advanced security visual analytics for multidimensional, temporal, and geo-spatial views of real-time security data capable of digesting structured and unstructured data analysis for system and security operation control center operators.

To develop and refine the modeling and systems necessary for much of the proposed research, there would also be a need for developing new simulation capabilities for the distribution grid that incorporate communications with devices/models for distribution control, distributed generation, storage, PEV, etc., to provide a representative environment for evaluating 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 evaluate their possible cross-impacts on each other.

8.6.5 Covert network channels in the Smart Grid: Creation, Characterization, Detection and Elimination

The idea of covert channels was introduced by Lampson in 1973 as an attack concept that allows for secret transfer of information over unauthorized channels. These channels demonstrate the notion that strong security models and encryption/authentication techniques are not sufficient for protection of information and systems. Earlier research on covert channels focused on multilevel, secure systems but more recently a greater emphasis has been placed on "covert network channels" that involve network channels and can exist in discretionary access control systems and Internet-like distributed networks. Given that many Smart Grid networks are being designed with Internet principles and technologies in mind, the study of covert network channels for the Smart Grid becomes an interesting research problem. Like the more general covert channels, covert network channels are typically classified into storage and timing channels. Storage channels involve the direct/indirect writing of object values by the sender and the direct/indirect reading of the object values by the receiver. Timing channels involve the sender signaling information by modulating the use of resources (e.g., CPU usage) over time such that the receiver can observe it and decode the information.

The concern over covert network channels stems from the threat of miscreants using such channels for communication of sensitive information and coordination of attacks. Adversaries will first compromise computer systems in the target organization and then establish covert network channels. Typically, such channels are bandwidth-constrained as they aim to remain undetected. Sensitive information that may be sent over such channels include Critical Energy Infrastructure Information (CEII), FERC 889 involving the leakage of operational information to power marketing entities, and cryptographic keying material that protects information and systems. In addition, information exchange for coordination of attacks such as management and coordination of botnets, and spreading worms and viruses are also important concerns.

For example, covert network channels have been created using IP communication systems by a variety of means including the use of unused header bits, modulating packet lengths, and modifying packets rates/timings. Similarly, such channels have been shown to be possible with routing protocols, wireless LAN technologies, and HTTP and DNS protocols. For the Smart Grid, an interesting research challenge is to identify new types of covert network channels that may be created. For example, given that the Smart Grid involves an extensive cyber-physical infrastructure, perhaps the physical infrastructure can be leveraged to design covert network channels. Additional challenges include identification of other covert network channels that can

be established on Smart Grid networks, for example, using relevant weaknesses in Smart Grid protocols. For all created channels, it is important to characterize the channels. This includes estimating channel capacity and noise ratios.

Covert channels can be detected at the design/specification level and also while they are being exploited. A variety of formal methods-based techniques have been developed in the past. An example is those based on information flow analysis. For runtime identification, several techniques specific to the type of covert network channel have been developed. Research challenges include identification of covert network channels for Smart Grid systems both at the design level and while they may be exploited. Once identified, the next challenge lies in eliminating them, limiting their capacity, and being able to observe them for potential exploitation. Means for doing so include the use of host and network security measures, and traffic normalization at hosts and network endpoints, such as firewalls or proxies. Again, research challenges include developing means for eliminating covert network channels, and in a case where that is not feasible, the objective is to limit their capacity and be able to monitor their use. Potential avenues of research include analyzing and modifying garbage collection processes in Smart Grid systems, and developing signature and anomaly-based detection techniques.

8.6.6 Denial of Service Resiliency

8.6.6.1 Overview

Smart Grid communications are progressing toward utilizing IP-based transport protocols for energy utility information and operational services. As IP-based nodes propagate, more opportunities for exploitation by miscreants are evolving. If a network component can be probed and profiled as part of the Smart Grid or other critical infrastructures, it is most likely to be targeted for some form of intrusion by miscreants. This is especially relevant with the growing use of wireless IP communications.

8.6.6.2 DoS/DDoS Attacks

Denial of Service and Distributed Denial of Service (DoS/DDoS) attacks have become an effective tool to take advantage of vulnerabilities. The attack objective is to take actions that deprive authorized individuals access to a system, its resources, information stored thereon, or the network to which it is connected.

A simple DoS attack attempts to consume resources in a specific application, operating system, or specific protocols or services, or a particular vendor's implementation of any of these targets to deny access by legitimate users. It may also be used in conjunction with other actions (attacks) to gain unauthorized access to a system, resources, information, or network.

The DDoS attack seeks to deplete resource capacity, such as bandwidth or processing power, in order to deny access to authorized users and can be levied against the infrastructure layer or the application layer. This technique utilizes a network of attack agents (a "botnet" comprised of systems that have had attack software installed surreptitiously) to amass a large, simultaneous assault of messages on the target. As with the DoS attack, DDoS may be combined with other techniques for malicious purposes.

IP-based networks are vulnerable to other attacks due to deficiencies of underlying protocols and applications. A man-in-the-middle, session-based hijack, or other technique may accompany the DoS/DDoS attack to inflict further damage on the target. Wireless networks in the AMI/HAN

environment can be difficult to secure and are of particular concern as the object of an attack or an entry point to the upstream network and systems.

8.6.6.3 Research and Development Requirements

The SGIP CSWG R&D subgroup desires to highlight and seek further research and development support in order to improve DoS/DDoS resiliency. We have identified the following areas of work as offering potential solutions worthy of further pursuit by Smart Grid stakeholders:

1. **Network architectures for survivability:** The Smart Grid networks and the public Internet will have several interface points which might be the target of DoS/DDoS attacks originating from the public Internet. A survivable Smart Grid network will minimize the disruption to Smart Grid communications, even when publicly addressable interfaces are subject to DDoS attacks;
2. **Policy-based routing and capabilities:** Policy-based routing is a fundamental redesign of routing with the goal of allowing communications if, and only if, all participants (source, receiver, and intermediaries) approve. A particular policy of interest for defending against DDoS attacks is the use of Capabilities. In this framework, senders must obtain explicit authorization (a capability) from the receiver before they are allowed to send significant amounts of traffic (enforced by the routing infrastructure). Smart Grid networks provide a good opportunity to design from the ground up a new routing infrastructure supporting capabilities;
3. **Stateless dynamic packet filtering:** Filtering and rate-limiting are basic defenses against DDoS attacks. We require further research in stateless packet filtering techniques to significantly reduce packet-processing overhead.

   An example of this is "Identity-Based Privacy-Protected Access Control Filter" (IPACF) which is advertised as having the "capability to resist massive denial of service attacks." IPACF shows promise for using "stateless, anonymous and dynamic" packet filtering techniques without IP/MAC address, authentication header (AH) and cookie authentication dependencies, especially for resource-constrained devices (RCDs).

   When compared to stateful filtering methods, IPACF may significantly reduce packet processing overhead and latencies even though it is dynamically applied to each packet. IPACF describes the ability to utilize discarded packets for real-time intrusion detection (ID) and forensics without false positives.

   Initial modeling reveals that embedded stateless packet filtering techniques may significantly mitigate DoS/DDoS and intrusion and could be evolved to defend man-in-the-middle attacks, while offering considerable device implementation options and economies of scale; and
4. **Lightweight authentication and authorization:** There is a distinct need for an embedded-level, lightweight, secure, and efficient authentication and authorization (AA) protocol to mitigate intrusion and DDoS attacks targeting resource-intense AA mechanisms. See Item 3 above.

8.6.7 Cloud Security

With the advent of cloud computing in the Smart Grid, special attention should be given to the use of cloud computing resources and the implications of leveraging those resources. There are several organizations that are focusing on security and appropriate use of cloud computing resources, including the Cloud Security Alliance. They have produced a document that addresses security areas for cloud computing that provides valuable guidelines to security in this environment. Work has also been done by NIST's cloud computing group that provides some guidelines for cloud computing use in government agencies.

As with any shared resource that will host potentially sensitive information, security mechanisms must be deployed that provide the appropriate protection and auditing capabilities throughout the cloud. Cloud computing must be evaluated with consideration of the unique constraints and consequences of control systems in the context of the Smart Grid. Impact of cloud provider engagement must also be considered in terms of liabilities for data existing in the cloud, in what is likely to be a multi-tenancy environment.

Data security issues must be addressed such as data ownership, data protection both in and out of the cloud for storage and transit, access control to the data and the cloud, and authorization considerations for trust and permissions. Trust models must be put in place to provide these guarantees in a manner that is verifiable and compliant with emerging regulations like NERC CIPs, FERC 889, user data privacy concerns, and other emerging compliance regulations. These types of regulations may have corollaries in industries like the health sector that could be considered, but differ enough that there are unique concerns.

WAN security and optimization issues must also be addressed depending on the data access patterns and flow of information in the cloud. This could include new work in encryption, key management, data storage, and availability model views. For instance, securely moving synchrophasor data from end nodes into the cloud on a global basis could be overly resource intensive. This might make real-time use infeasible with current cloud computing technology without further research in this area. Current distributed file system approaches may not be appropriately optimized to operate in a secure WAN environment, favoring network-expensive replication in a LAN environment as a trade-off for speed.

8.6.8 Security Design & Verification Tools (SD&VT)

Complexity breeds security risks. This is most evident with the Smart Grid, as it is a collection of many complex, interconnected systems and networks that represent a fusion of IT, telecommunications, and power system domains. Each of these domains represents distinct forms of technology and operations that have unique interdependencies on each other and can indeed lead to elements of the cyber system (i.e., IT and communications) impacting the reliability of elements of the power system and vice-versa.

Correctly designing security for each of the domains is primarily done from the perspective of only the power or cyber domain. For example, designing certain security controls (without an adequate understanding of an overall power system context) to prevent excessive failed authentication attempts by lockout on a communication/control device might in fact create a denial of service condition that is more likely to degrade the reliability of the broader system than mitigate the original security risk that one was trying to address. System-wide security design and implementation is not commonly done using formal methods that can be verified, nor

can it give any deterministic analysis of expected performance or behavior for given system states, faults, or threat events.

Research and development should be conducted into SD&VT that can—

a. Formally model Smart Grid cyber and power systems, their interactions, and their underlying components using a formal language. Candidates for examination and further adaptation can include: UML, Formal ontologies and knowledge representation based on semantic Web technologies such as OWL, or other novel forms. The language should allow one to communicate certain assertions about the expected function of a device/system and its security controls and risks, as well as the relationship between components, systems, and system communication. Most importantly, the model must provide a basis to represent multiple concurrent and independently interacting complex states;

b. Provide automatic, intelligent methods of verification that discover reliability and security issues in component and system states for the Smart Grid, in a formal design model (as represented using the methods in (a.) using any number of machine learning or knowledge/logic inference techniques; and

c. Simulate any number of scenarios based on the intelligent model built using (a.) and (b.), and provide predictive analytics that can optimize a security design that minimizes risks and costs, as well as maximizing security and reliability in the power and cyber domain.

8.6.9 Distributed versus Centralized Security

Several models for designing intelligent and autonomous actions have been advanced for the Smart Grid, particularly in automated distribution management. Several models have also been deployed in the advanced metering space, where, for example, there is ongoing debate regarding the functions and processing which should be carried out by the meter, versus centralized systems (such as Meter Data Management or Load Control applications in the Control Center). Some approaches offer embedded security controls, while some externalize security and some offer combinations of both approaches. In the larger context of advanced distribution automation, there is a similar debate regarding how much "intelligence" should be deployed within IEDs, distributed generation endpoints, etc., versus reliance on centralized systems.

Also, Wide Area Situational Awareness (WASA) systems and actors are distributed by nature, yet most security mechanisms in place today are centralized. What is an appropriate security mechanism to place in a distributed environment that will not compromise an existing security framework, yet allow third-party WASA systems and actor's visibility into security intelligence, as well as allow appropriate functional capability to act and respond to distributed security events?

We propose advanced security research be conducted to determine an underlying security model to support these various approaches to distributed versus centralized security intelligence and functionality in the grid. Some factors to consider include the following:

- Communication with centralized security mechanisms may be interrupted. Research should be conducted into hybrid approaches and the appropriate layering of security controls between centralized and distributed systems. For example, centralized security

- Externalized security mechanisms, such as in some control system protocol implementations (e.g., ANSI C12.22), may be desirable because they can be scaled and upgraded independently in response to evolving threats and technology changes, possibly without retrofitting or upgrading (perhaps millions of) devices deployed in the field. On the other hand, some mechanisms should be deployed locally, such as bootstrap trusted code verification modules for firmware, logging, etc. Research should be conducted in best practices to determine the appropriate model for deployment.
- Rapid changes of cryptographic keys and authentication credentials may be needed to contain security incidents or provide ongoing assurance, and centralized security systems may be needed. Would a distributed or centralized model be more efficient and secure?
- Functionality of some components (e.g., breakers, IEDs, relays, etc.) and communications functions should not fail due to failure of a security mechanism. Is a distributed model appropriate for WASA?
- Integration of security mechanisms between security domains is needed (for example, between logical and physical security mechanisms of remote sensors). How does a distributed vs. centralized model effect the integration?
- Edge devices such as distributed generation controllers and substation gateways need to be capable of autonomous action (e.g., self-healing), but these actions should be governed by business rules and under certain circumstances data from the devices should not be trusted by decision support systems and systems that have more than local control of the grid. Does a distributed model manage edge devices more efficiently and securely than a centralized model?
- A trust model is needed to govern autonomous actions, especially by systems outside the physical control of the utility. Will there be a centralized trust model or will the industry evolve to a distributed trust model allowing numerous Smart Grid actors to interact trustfully in regards to security interactions?
- Do distributed or centralized trust models force over-reliance by control systems support groups on IT groups?

While it is not be clear which security functions should be centralized or decentralized for a particular implementation, research into coherent reference models and taxonomies for layering these controls following best practice should be conducted. The model should contain a standard approach by which Smart Grid actors can make better security architecture decisions based on risks to their environment and efficiencies of security operations.

8.6.10 System Segmentation and Virtualization

The first principles of cyber security are isolation and defense-in-depth. The objective of this research is to develop methods to protect network end-points through Intense System Segmentation. The research should seek to create a platform that implements the characteristics of time-tested and recognized security principles. These principles include isolation, a minimal trusted computing base, high usability and user transparency, a limited privilege capability that

provides for user, process, and application class of service definitions, and a default-deny rules engine enforcing such privileges.

The requirement for continuous availability of Utility Grid operations necessitates a high degree of reliability within and across domains. Many domain end-points, such as legacy substation equipment, rely on outdated operating systems with little or no encryption capabilities, posing numerous challenges to the overall security of the Smart Grid. By enclosing an Intense System Segmentation framework around the existing computer architecture of these localized end-points, the legacy infrastructure should gain a layer of redundancy and security. Intense System Segmentation within a single Virtual Machine (VM) should provide granular isolation to reduce the attack surface to a single file and/or single application, and reduce the ability of threats to virally propagate. End-point protection must also be customizable to address the specific needs of subsectors within individual Energy Sector Domains.

Traditional virtualization techniques that use sandboxing have known, exploitable vulnerabilities. This is largely the result of the communication that traditional VMs require in order to perform sharing functions between applications and administrative requirements. Sandboxing also relies on binary decisions for processes and communication that might compromise security. Intense System Segmentation should allow communication between isolated environments to occur while eliminating any execution of code outside of an isolated environment. An Intense System Segmentation platform may use some of the tools of virtualization, such as a sealed hypervisor to provide protection of end-point resources, and sealed VMs to perform computing in intense isolation. Hypervisors are designed to streamline communication between a wide range of applications and processes, and utilize APIs and other communication entry points. A sealed hypervisor should block these communication entry points, for both the hypervisor and an attestable kernel.

Maintaining the resiliency and continuous availability of the power grid should be one of the primary goals in creating a system segmentation platform. As this platform assumes that end-points will be penetrated, secure recovery, containment, and resiliency should be a focus of continued research. The inherent redundancy of hypervisor-driven segmentation can be utilized to enclose legacy systems and should allow customizable interoperability between the DHS-defined critical infrastructure sectors. An open platform that uses a secure computing architecture and leverages the tools of virtualization will enhance the resiliency of existing Energy Sector critical infrastructure. The use of virtualization has also been recognized as building block to implement resiliency through agility (a “moving target” paradigm). This can be used to increase uncertainty and cost to attackers. Thus this research should help to leverage “moving target” paradigm in Smart Grid systems as well as improving security of Smart Grid legacy systems.

8.6.11 Vulnerability Research

Vulnerabilities may be caused by many things in computer devices. Poor coding is the primary cause of vulnerabilities in computer systems today, but physical attacks have much higher value in Smart Grid devices than in standard computing environments. Both design and implementation vulnerabilities represent varying and potentially great risks to the power grid. While future code revisions and hardware versions may introduce new vulnerabilities, many vulnerabilities may exist in the current systems that require significant time to identify and address. For many years, SCADA systems have been quarantined from security scans for fear of

causing outages. While care and prudence should be taken with critical systems, the fragility of these systems represents a great existing risk to the grid. Newer Smart Grid systems such as advanced metering infrastructure, hybrid/electric vehicles and supporting infrastructure, and demand response all represent new unknowns. A few significant projects have undertaken security research on some of these devices, and positive results have resulted but more research is necessary. Security research grants are key to ensuring greater scrutiny of the existing systems to find vulnerabilities that may currently exist in Smart Grid equipment.

8.6.12 Vulnerability Research Tools

Smart Grid networks represent a great deal of proprietary, obtuse systems and protocols. Before security can be reasonably well tested, tools must be created to maximize the value of security research. Several freely available tools have already been in active development but lack resources. Other tools are important but nonexistent.

Examples of existing security research tools include:

- GoodFET—Hardware analysis tool allowing debugging of numerous platforms/chipsets, largely focused on the predictability of power-glitching to bypass hardware security mechanisms; http://goodfet.sourceforge.net/
- KillerBee—ZigBee® analysis tool allowing for capture and analysis of ZigBee® networks and interaction with devices.

Examples of security research tools yet to be started:

- Devices to easily interact with, capture, and analyze traffic of metering networks for different vendors. Currently, the best toolset available is the software-defined radio named USRP2 from Ettus Research, costing roughly $2k. This toolset allows for RF analysis and indeed can capture data bits. However, the ideal toolset would allow an analyst's computer to interface to the metering networks and provide an appropriate network stack in a popular operating system such as Linux. The tools would allow the customers (mostly IOU's due to funding) to perform their own security research against the platforms, and allow them to validate their own security;
- Open-source Protocol analysis tools, such as the protocol parsers included in the open-source tool Wireshark. Protocols like IEC61850, IEC61968/ANSI C12.*, proprietary AMI protocols, DNP3, Modbus, and other popular power grid protocols being included in the Smart Grid should be freely available for analysis by asset-owners and researchers; and
- Firmware analysis tools that can be configured to understand address/IO mapping and input vectors, and can identify potential vulnerabilities for a given platform.

8.6.13 Data Provenance

We cannot assume that the Smart Grid will never be compromised. Once we assume that there are insiders who have access, operational data can no longer be trusted. In addition, while traditional security-related protocols reject data if the security fails, we cannot afford to ignore operational data because the data is suspect.

Therefore, we need methods to deal with such data while maintaining the operational integrity and state of many systems. Some of the issues include:

- Measuring the quality of the data from a security perspective. This may include both subjective and objective viewpoints, and may have to deal with uncertainty about the data.
- How do we make operational decisions based on data that may have questionable attributes of confidentiality, integrity, authenticity, non-repudiation, and timeliness?
- How do organizations coordinate their beliefs with other organizations? What happens if the other organizations are suffering from a significant security breach? How should one organization react with data of uncertain trustworthiness?

8.6.14 Security and Usability

One of the issues with the implementation of security is the usability of security, or the ease of use and impact on convenience. Some organizations weaken their security for various reasons (e.g., operational cost, profit, effort, lack of understanding). To encourage users to deploy strong security, certain issues must be overcome. These include:

- Security must be self-configuring. That is, the systems should be able to configure themselves to maximize security without requiring expert knowledge of security.
- Security options should be simple and understandable by users who lack a background in security. Concepts like certificates and keys are not well understood by end users. These details should be hidden.
- The relationship between a security policy, the protection the policy provides, and the security configuration should be clear. If a system is "misconfigured" in a way that reduces the protection, the risk should be clear to the user.
- Security should be reconfigured. In other words, if a policy is changed (for instance, stronger security is enabled), the systems should adapt to meet the new requirements. It should not be necessary to physically visit devices to reconfigure them. However, if policy changes, some devices might be unable to change, and end up being isolated from the new configuration. How can the user minimize the disruption?
- Part of usability is maintainability. There needs to be ways to upgrade security without replacing equipment. Firmware upgrades are often proprietary, vendor-specific, and have uncertain security. How can a vendor best plan their migration strategy between security revisions and major policy changes?

Usability of security technologies needs to improve to address these issues.

8.6.15 Cyber Security Issues for Electric Vehicles

PEVs have a similar entry point to the electric grid as the smart meters. Thus, they are associated with largely the same security and privacy issues. When PEVs connect to the grid to charge their batteries, it is necessary to communicate across a digital network to interface with a payment and settlement system. Assuming that proper standards are adopted, these charging solutions will have the same issues as payment and settlement systems for other products. Appropriate physical security measures and tamper-evident mechanisms must be developed to prevent or detect the

insertion of "cloning" devices to capture customer information and electric use debit and credit information. One may expect that miscreants will develop means to clone legitimate PEV interfaces for criminal activity.

It has been reported that a terminated employee from a car dealership logged into the company's Web-based system and was able to remotely wreak havoc on more than 100 vehicles. The dealership's system was able to disable the starter system and trigger incessant horn honking for customers that have fallen behind on car payments as an alternative to repossessing the vehicle. It is necessary to develop mechanisms that make sure car buyers are properly informed and fully protected.

Like other areas that depend on a supply chain, PEVs have similar issues. Thus, it is necessary to make sure that car repair shops will not be able to install illegal devices at time of car maintenance.

Utilities and private/public charging stations may also be subject to law enforcement search warrants and subpoenas in regards to PEV usage. A PEV may be stolen and used in the act of a crime. Law enforcement may issue an "alert" to control areas to determine if the suspected PEV is "connected" to the grid and would want to know where and when. Research may also be requested by law enforcement to enable a utility to be able to "disable" a PEV in order to preserve evidence and apprehend the criminals.

8.6.16 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 include:

- Connection/disconnection information reported by meters may identify an unauthorized disconnect, which in the context of 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.

Related prior work includes fraud detection algorithms and models that are being used in the credit card transactions.

CHAPTER NINE
OVERVIEW OF THE STANDARDS REVIEW

9.1 OBJECTIVE

The objective of the standards review is to ensure that all standards applicable to the Smart Grid adequately address the cyber security requirements included in this report. If the standards do not have adequate coverage, this review will identify those where changes may need to be made or where other standards may need to be applied to provide sufficient coverage in that area.

The CSWG has worked closely with the standards bodies to identify the standards for review and to gain appropriate access to the standards. This will be an ongoing effort as there are many standards that apply and must be assessed. To initiate the process, the CSWG established a standards subgroup to perform the assessments. The standards subgroup will begin with the standards identified in the NIST Framework document[9] and will continue to refine the process as more standards are identified for assessment.

9.2 REVIEW PROCESS

The standards subgroup will review, assess, and report on the cyber security coverage of each of the standards identified in the NIST Framework document. The list for initial review was agreed upon by the participating standards bodies and the NIST Smart Grid team.

The review process ensures that each standard will be reviewed by multiple reviewers from the standards subgroup. Each standard will be reviewed by a minimum of the following:

- 2 General (cross-industry) reviewers
- 1 IT/Telecom sector reviewer
- 1 electric sector reviewer

The reviewers will perform the reviews of each standard independently and provide an assessment via the standards assessment template [*See* Table 9-1]. This review will include the following:

- Map to Smart Grid cyber security requirements [*See* §3.5]
- Identification of Issues/Gaps/Alternatives/Action Items

When assessments by all reviewers of the standard are completed, they will be reviewed to determine if they are consistent across reviewers or if conflicts between reviewers exist. Where reviews are found to be consistent, the assessment will be consolidated and submitted to the NIST management for further review.

After the CSWG review, all assessments will be submitted for inclusion in a forthcoming separate NIST document titled *Summary of Use, Application, Cybersecurity, and Functionality of Smart Grid Interoperability Standards Identified by NIST.*

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

9.3 NIST CSWG STANDARDS ASSESSMENT TEMPLATE

The following table presents the standards assessment template used by the standards subgroup to report findings from their standards review effort.

The section of the template appearing in gray highlight will be repeated as needed within the standard. Some standards may have many sections that will be included in the assessment template.

In the template, the NISTIR Security Family will include the name of that requirements family as identified in Chapter 3, such as "Incident Response."

If Cryptography is included in the standard being reviewed, this standard will be referred for further review to the Cryptography and Key Management subgroup.

If another standard is referenced in the standard being reviewed, the standard will be identified as needing further review, and the referenced standard will be obtained for review by the standards subgroup.

Table 9-1 CSWG Standards Assessment Template

Standard number and version:
Standard Name:
Does the standard cover cyber security? (Y/N): If "No," should it? (Y/N):
Describe any gap(s) in coverage:
Standard section/chapter/page reference:
Applicable NISTIR security family:
Applicable NISTIR requirement:
Does the standard meet the security requirement? (Y/N or P-Partial) If No or Partial, what is the gap? Should the standard or the NISTIR be revised? If yes, what is the recommended revision? Is security for this standard covered elsewhere? (Y/N) If Yes, where?
Is crypto included in the standard? (Y/N) If No, should it? (Y/N) If Yes, provide detail on cryptography Describe Algorithm, Mode, Key Size, etc. Does the cryptography meet the security requirement? (Y/N or P-Partial)
List any referenced standards:

9.4 STANDARDS REVIEW LIST

The first list of standards that will be reviewed were selected in the NIST Framework document process. As indicated in the objective above, the standards review process will continue as more standards are identified for review and assessment. The assessments will appear in a separate document; please refer to the forthcoming *Summary of Use, Application, Cybersecurity, and Functionality of Smart Grid Interoperability Standards Identified by NIST* for more detail on the standards and their current assessments.

CHAPTER TEN
KEY POWER SYSTEM USE CASES FOR SECURITY REQUIREMENTS

The focus of this chapter is to identify the key Use Cases that are "architecturally significant" with respect to security requirements for the Smart Grid. This identification is neither exhaustive nor complete. New Use Cases may be added to this appendix in future versions of this report as they become available. The Use Cases presented in this appendix will be employed in evaluating Smart Grid characteristics and associated cyber security objectives; the high-level requirements of confidentiality, integrity, and availability, (CI&A); and stakeholder concerns. The focus here is more on operational functions rather than "back office" or corporate functions, since it is the automation and control aspects of power system management that are relatively unique and certainly stretch the security risk assessment, security controls, and security management limits.

Many interfaces and "environments"—with constraints and sensitive aspects—make up the information infrastructure that monitors and controls the power system infrastructure. This chapter does not directly capture those distinctions, but leaves it up to the implementers of security measures to take those factors into account.

10.1 USE CASE SOURCE MATERIAL

The Use Cases listed in this chapter were derived "as-is" from a number of sources and put into a common format for evaluation. The resulting list presented in this appendix does not constitute a catalog of recommended or mandatory Use Cases, nor are the listed Use Cases intended for architecting systems or identifying all the potential scenarios that may exist. The full set of Use Cases presented in this chapter was derived from the following sources:

- **IntelliGrid Use Cases**: Over 700 Use Cases are provided by this source, but only the power system operations Use Cases and Demand Response (DR) or Advanced Metering Infrastructure (AMI) cases are of particular interest for security. The Electric Power Research Institute (EPRI) IntelliGrid project developed the complete list of Use Cases. *See* IntelliGrid Web site, Complete List of Power System Functions.
- **AMI Business Functions**: Use Cases were extracted from Appendix B of the Advanced Metering Infrastructure Security (AMI-SEC) System Security Requirements document (published by the AMI-SEC Task Force) by the Transmission and Distribution Domain Expert Working Group (T&D DEWG), and the Smart Grid Interoperability Panel – Cyber Security Working Group (SGIP-CSWG) has now also posted this material on the SGIP TWiki).
- **Benefits and Challenges of Distribution Automation**: Use Case Scenarios (White Paper for Distribution on T&D DEWG), extracted from a California Energy Commission (CEC) document which has 82 Use Cases; now posted on the SGIP TWiki.
- **EPRI Use Case Repository**: A compilation of IntelliGrid and Southern California Edison (SCE) Use Cases, plus others. *See* EPRI Web site, Use Case Repository.
- **SCE Use Cases**: Developed by Southern California Edison with the assistance of EnerNex. *See* SCE.com Web site, Open Innovation.

A certain amount of overlap is found in these sources, particularly in the new area of AMI. However, even the combined set (numbering over 1000 Use Cases) does not address all requirements. For example, for one operation—the connect/disconnect of meters—6 utilities developed more than 20 use case variations to meet their diverse needs, often as a means to address different state regulatory requirements.

The collected Use Cases listed in this chapter were not generally copied verbatim from their sources but were oftentimes edited to focus on the security issues.

10.2 KEY SECURITY REQUIREMENTS CONSIDERATIONS

The Use Cases listed in subsection 11.3 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 in the three principal areas addressed in subsections 11.2.1 through 11.2.3.

10.2.1 CIA Security Requirements

The following points briefly outline security requirements related to confidentiality, integrity, and availability.

Confidentiality is generally the least critical for power system reliability. However, this is important as customer information becomes 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.

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

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

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

- 4 milliseconds for protective relaying,
- Subseconds for transmission wide area situational awareness monitoring,
- Seconds for substation and feeder supervisory control and data acquisition (SCADA) data,
- Minutes for monitoring noncritical 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.

10.2.2 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 24×7 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.

10.2.3 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 ICIA) 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 (RBAC) 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 bypassing 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 reassessment of security risks

10.3 USE CASE SCENARIOS

The following subsections present the key Use Cases deemed architecturally significant with respect to security requirements for the Smart Grid, with the listing grouped according to 10 main categories: AMI, Demand Response, Customer Interfaces, Electricity Market, Distribution Automation, Plug-in Hybrid Electric Vehicles (PHEV), Distributed Resources, Transmission Resources, Regional Transmission Operator / Independent System Operator (RTO/ISO) Operations, and Asset Management.

10.3.1 AMI Security Use Cases

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 that 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 distributed energy resources (DER) and plug in electric vehicle (PEV)

Feed-In Tariff Metering for DER and PEV

Bill - Paycheck Matching

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	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	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: AMI

Scenario: Prepaid 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 that 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 prepayment 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 prepayment. 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

Nontechnical losses (or theft of power by another name) have long been an ongoing battle between utilities and certain customers. In a traditional meter, the meter reader 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 that 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 Nonpayment

Remote Disconnect for Emergency Load Control

Unsolicited Connect / Disconnect Event

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 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	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 (CIS), the Trouble Call System (TCS), Geographical Information System (GIS), and the Outage Management System (OMS) 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 that 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

Geolocation of meter

Smart meter battery management

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers	Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions	Customer data privacy and security
Accommodates all generation and storage options	Availability is important, but only in terms of hours or maybe days	Retail Electric Supplier access
Enables new products, services and markets	Confidentiality is not important unless some maintenance activity involves personal information	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	Objectives/Requirements	Potential Stakeholder Issues
Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	To reduce energy theft To prevent theft/compromise of passwords and key material To prevent installation of malware	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	Objectives/Requirements	Potential Stakeholder Issues
Optimizes asset utilization and operate efficiently	To reduce theft	Customer data privacy and security
Operates resiliently against attack and natural disasters	To protect integrity of reporting	Retail Electric Supplier access
	To maintain availability for reporting and billing	Customer data access
		Customer Safety

10.3.2 Demand Response Security Use Cases

Category: Demand Response (DR)

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. RTP 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 RTP 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 RTP 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 24×7 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 nonrepudiation, of pricing information is critical, since there could be large financial and possibly legal implications Availability, including nonrepudiation, 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 TOU pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

TOU 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 RTP is more flexible than TOU, 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 TOU tariffs are employed.

Today larger commercial and industrial (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 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, 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: 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 TOU 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	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: Demand Response

Scenario: Mobile Plug-In Electric Vehicle 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

10.3.3 Customer Interfaces Security Use Cases

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 (HANs) and/or building energy management (BEM) 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 HANs and/or BEM 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, prepaying 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

10.3.4 Electricity Market Security Use Cases

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 subsection 10.3.2, is a part of the electricity market.

Scenario Description

The bulk power market varies from region to region, and is conducted primarily through RTOs and ISOs. 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 subsection 10.3.2, 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 subsection (see 10.3.2).)

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: 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 subsection 10.3.2, 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	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

10.3.5 Distribution Automation Security Use Cases

Category: Distribution Automation (DA)

Scenario: DA within Substations

Category Description

A broad definition of "distribution automation" includes any automation that 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, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain DA functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other DA 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 supervisory control and data acquisition (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: DA Using Local Automation

Category Description

A broad definition of “distribution automation” includes any automation that 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, 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 that 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: DA Monitoring and Controlling Feeder Equipment

Category Description

A broad definition of “distribution automation” includes any automation that 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, 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

Automate emergency response

Provide 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 that 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, 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 become increasingly critical.

The automated fault location, isolation, and restoration (FLIR) 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	Integrity of outage information is critical	Customer safety
Optimizes asset utilization	Availability to detect large-scale outages usually involve multiple sources of information	Customer device standards
Anticipates and responds to system disturbances	Confidentiality is not very important	Demand response acceptance by customers

Category: Distribution Automation

Scenario: Load Management

Category Description

A broad definition of "distribution automation" includes any automation that 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, 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 precooling, heat storage management).

Direct load control and load shedding

Demand side management

Load shift scheduling

Curtailment planning

Selective load management through HANs

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, 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 (DMS) 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 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	Integrity is critical to operate the distribution power system reliably, efficiently, and safely	Customer safety
Optimizes asset utilization	Availability is critical to operate the distribution power system reliably, efficiently, and safely	Customer device standards
Anticipates and responds to system disturbances	Confidentiality is not important	Demand response acceptance by customers

Category: Distribution Automation

Scenario: Distributed Energy Resources 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 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

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

Category: Distribution Automation

Scenario: Distributed Energy Resource 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, 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 term 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	Integrity not critical due to multiple sources of data	Cyber security
Optimizes asset utilization	Availability is not important	
Anticipates and responds to system disturbances	Confidentiality is not important	

10.3.6 PHEV Security Use Cases

Category: Plug In Hybrid Electric Vehicles (PHEV)

Scenario: Customer Connects PHEV 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

Scenario: Customer Connects PHEV 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

Scenario: PHEV 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 consumers	Improved system stability and availability	Vehicle standards
Accommodates all generation and storage options	To keep customer information private	Customer safety
Enables new products, services and markets	To insure DR messages are accurate and trustworthy	Customer device standards
Provides power quality for the digital economy		Demand response acceptance by customers
Optimizes asset utilization and operate efficiently		

Category: Plug In Hybrid Electric Vehicles

Scenario: PHEV 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	Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers	Improved system stability and availability	Vehicle standards
Accommodates all generation and storage options	Pricing signals are accurate and trustworthy	Customer safety
Enables new products, services and markets	Customer information is kept private	Customer device standards
Provides power quality for the digital economy		Demand response acceptance by customers
Optimizes asset utilization and operate efficiently		

10.3.7 Distributed Resources Security Use Cases

Category: Distributed Resources

Scenario: Customer Provides Distributed Resource

Category Description

Traditionally, distributed resources have served as a primary or emergency backup 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 backup 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	Commands are trustworthy and accurate	Safety
Accommodates all generation and storage options	Customer's data is kept private	Customer data privacy and security
Enables new products, services and markets	DR messages are received timely	
Provides power quality for the digital economy		
Optimizes asset utilization and operate efficiently		

10.3.8 Transmission Resources Security Use Cases

Category: Transmission Operations

Scenario: Real-Time Normal Transmission Operations Using Energy Management System (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 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 EMS. 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	Integrity is vital to the safety and reliability of the transmission system	Customer safety
Optimizes asset utilization	Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s)	Customer device standards
Anticipates and responds to system disturbances	Confidentiality is not important	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 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

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 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 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 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, load tap changer (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	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., 1 s) Confidentiality is not important	Customer safety 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 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 synchrophasor 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 is 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., 1 s) Confidentiality is not important	Cyber Security Customer data privacy and security

10.3.9 RTO/ISO Operations Security Use Cases

Category: RTO/ISO Operations		
Scenario: RTO/ISO Management of Central and DER Generators and Storage		
Category Description TBD		
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 nonmarket 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

10.3.10 Asset Management Security Use Cases

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 Offline and Online 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, 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 online condition monitoring devices for the range of assets monitored, offline test results, mobile work force technologies, the communications equipment used to collect the online 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, 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 data 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, 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 online condition monitoring devices for the range of assets monitored, offline test results, mobile workforce technologies, the communications equipment used to collect the online 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 F:
LOGICAL ARCHITECTURE AND INTERFACES OF THE SMART GRID

The following subsection refers to detailed logical interfaces including both diagrams and tables that allocate the logical interfaces to one of the logical interface categories.[10]

F.1 ADVANCED METERING INFRASTRUCTURE

The advanced metering infrastructure (AMI) consists of the communications hardware and software, together with the associated system and data management software, that creates a bi-directional network between advanced metering equipment 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 with real-time (or near-real-time) pricing of electricity and may help utilities achieve necessary load reductions. Figure F-1 diagrams the AMI, and Table F-1 lists the AMI logical interfaces by category.

[10] Please note that during development, logical interface 23 was deleted. Subsequent interfaces were not renumbered due to the amount of development already done at that time. It is expected that this will be resolved in the next version of this document.

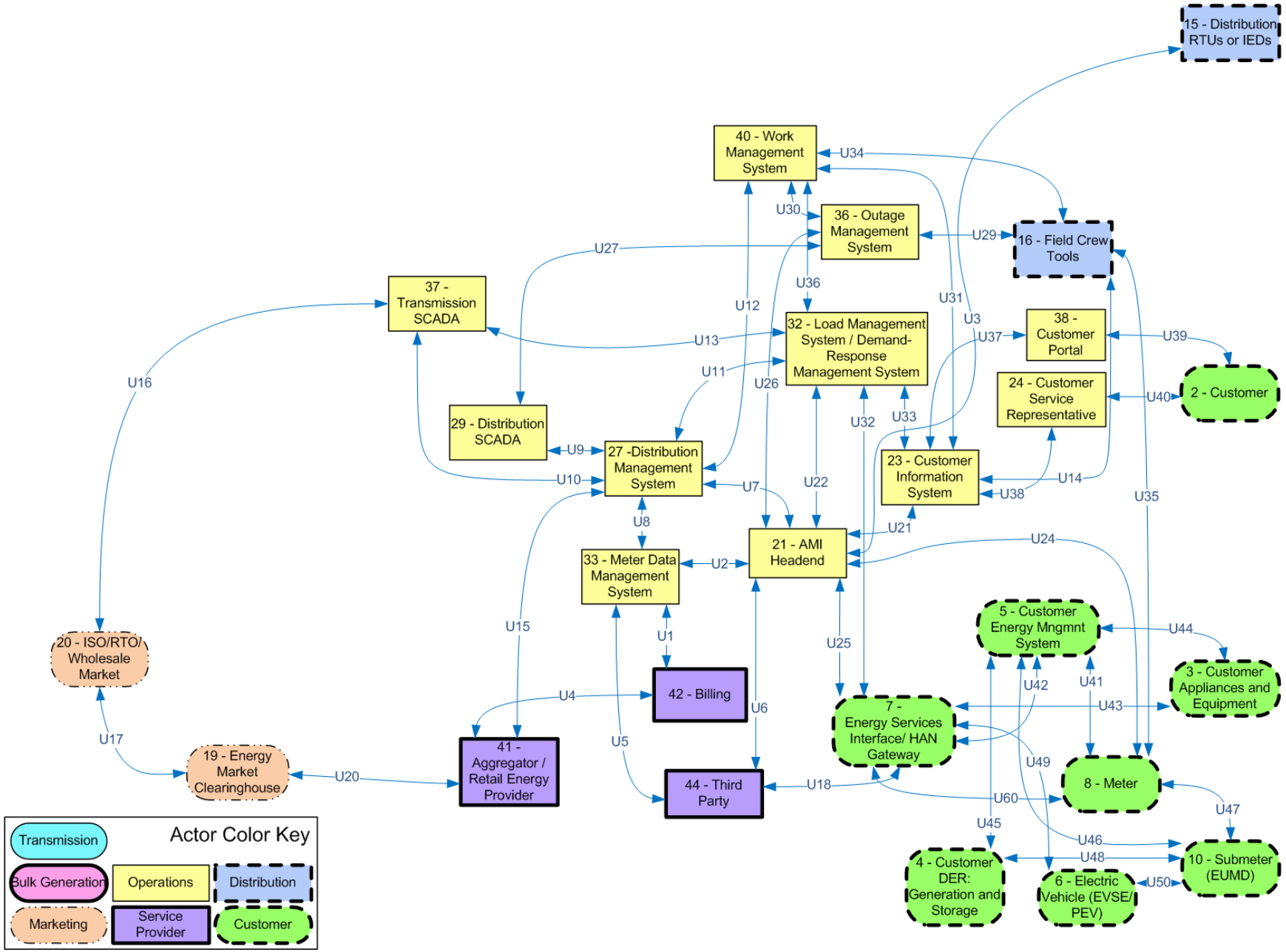

Figure F-1 Advanced Metering Infrastructure

Table F-1 AMI Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. 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
2. 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	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. 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	
5. 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
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U7, U10, U13, U16
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U22, U26, U31
8. 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
9. Interface with B2B[11] connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U17, U20
10. 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

[11] B2B – Business To Business

Logical Interface Category	Logical Interfaces
11. 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
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U8, U21, U25, U32
14. 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	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV[12]	U43, U44, U45, U49
16. 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
17. 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
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41, U46, U47, U50
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. 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
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	U5, U132

[12] PEV-Plug in Electric Vehicle

Logical Interface Category	Logical Interfaces
22. 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

F.2 DISTRIBUTION GRID MANAGEMENT

Distribution grid management (DGM) focuses on maximizing the 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 DGM include increased reliability, reductions in peak loads and improved capabilities for managing distributed sources of renewable energy. Figure F-2 diagrams the DGM, and Table F-2 lists the DGM logical interfaces by category.

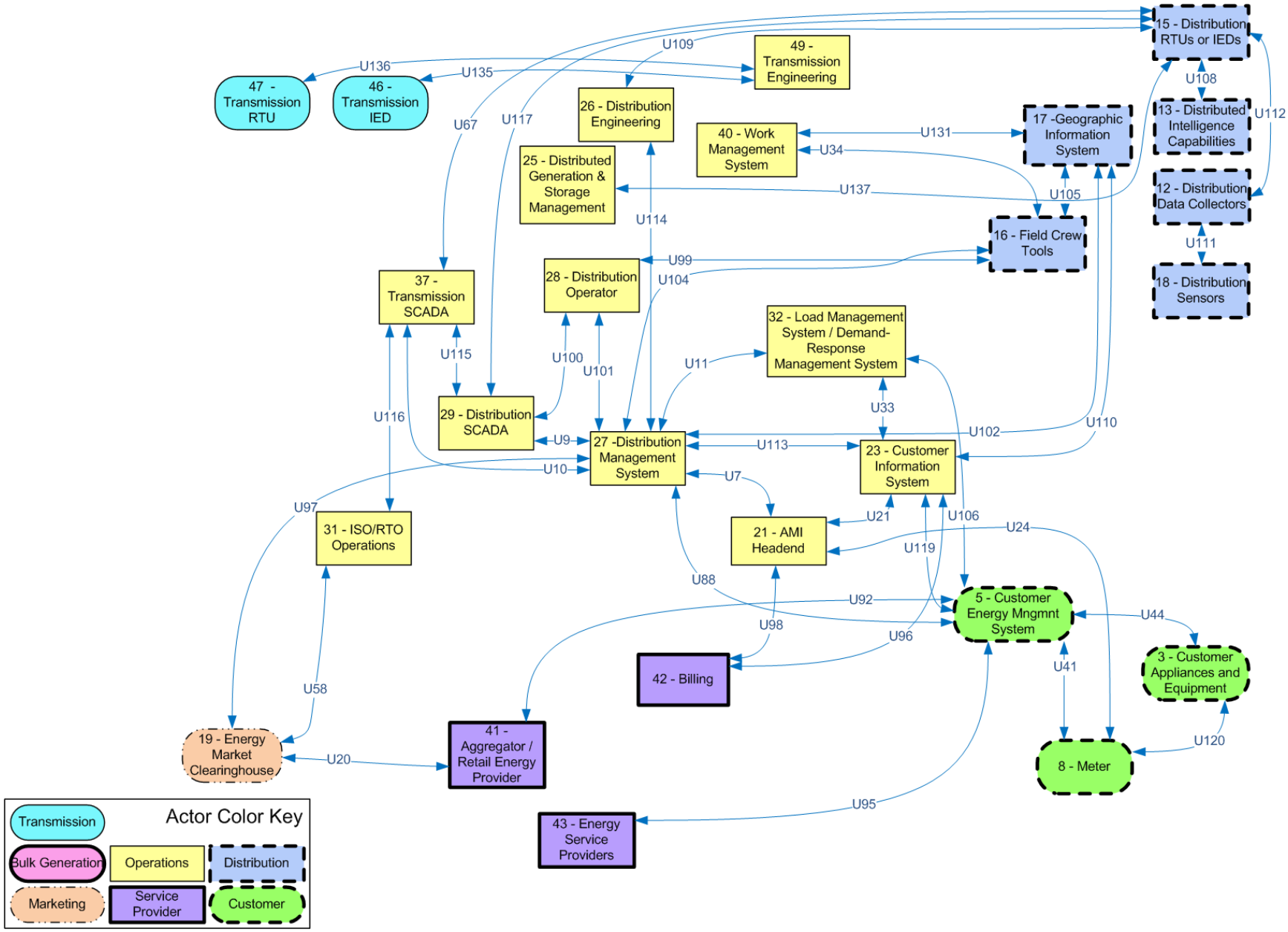

Figure F-2 Distribution Grid Management

Table F-2 DGM Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. 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, U135, U136
2. 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	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. 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	
5. 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
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U7, U10, U115, U116
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U96, U98, U110
8. 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
9. 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
10. 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
11. 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
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	U108, U112

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U95, U119
14. 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	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U44, U120
16. 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
17. 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
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. 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
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. 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

F.3 ELECTRIC STORAGE

Electric storage (ES) is the means of storing energy either directly or indirectly. The significant bulk of energy storage technology available today is pumped hydro-electric storage hydroelectric technology. New storage capabilities, especially in the area of distributed storage, would benefit the entire grid in many aspects. Figure F-3 shows the ES diagram, and Table F-3 lists the associated ES logical interfaces by category.

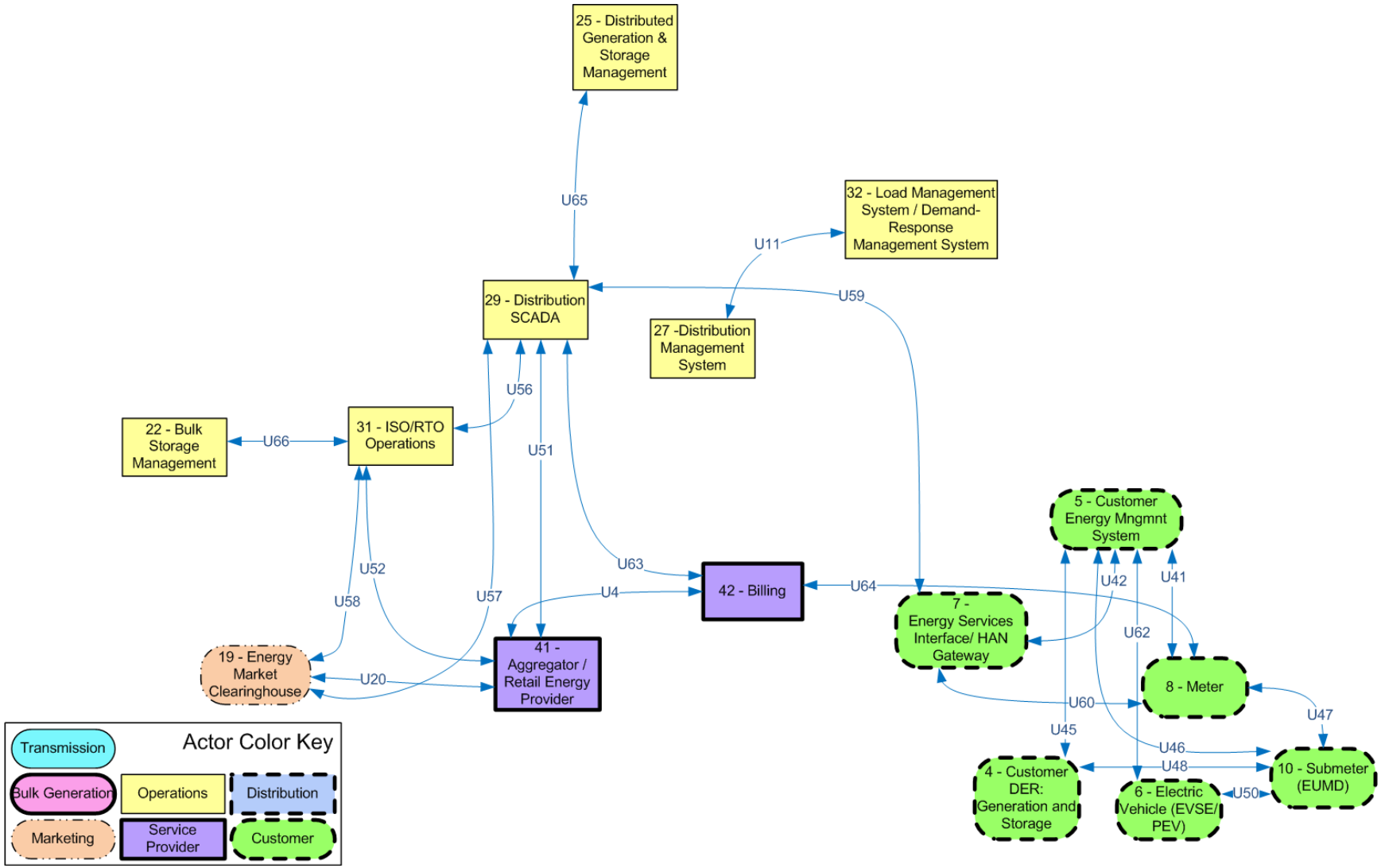

Figure F-3 Electric Storage

Table F-3 ES Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. 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
2. 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	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. 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	
5. 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
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U56
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U63
8. 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
9. 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
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U59
11. 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
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	None
14. 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	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U42, U45, U62
16. 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
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U41, U46, U47, U48, U50, U64
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. 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
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. 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

F.4 ELECTRIC TRANSPORTATION

Electric transportation (ET) refers primarily to enabling large-scale integration of PEVs. Electric transportation will 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 F-4 and Table F-4 address the ET logical interfaces.

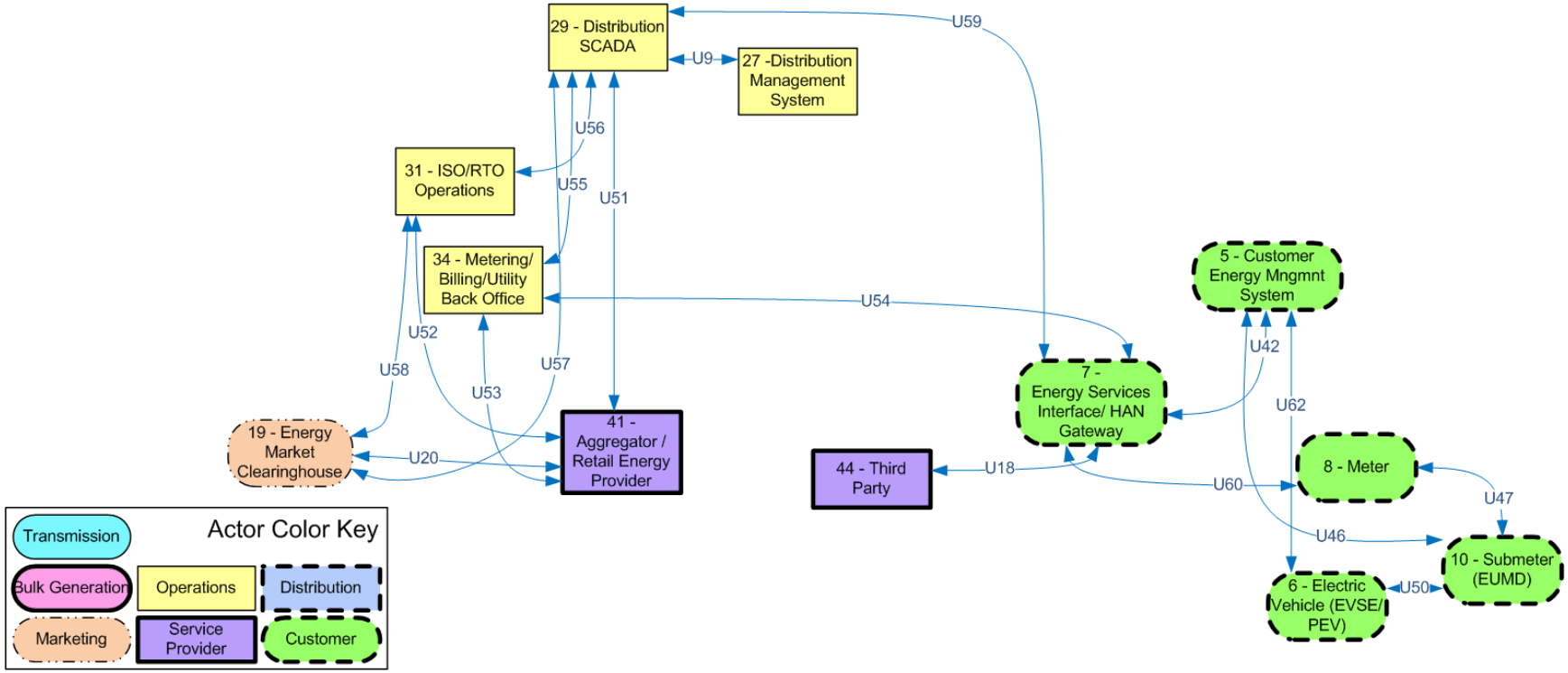

Figure F-4 Electric Transportation

Table F-4 ET Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. 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
2. 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	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. 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	
5. 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
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U56
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	None
8. 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
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U20, U51, U52, U53, U57, U58
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U59
11. 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

Logical Interface Category	Logical Interfaces
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	None
14. 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	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U62
16. 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
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U46, U47, U50, U54, U60
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. 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
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. 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

F.5 CUSTOMER PREMISES

The customer premises address demand response (DR) 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. Figure F-5 diagrams the customer premises and Table F-5 provides the companion list of customer premises.

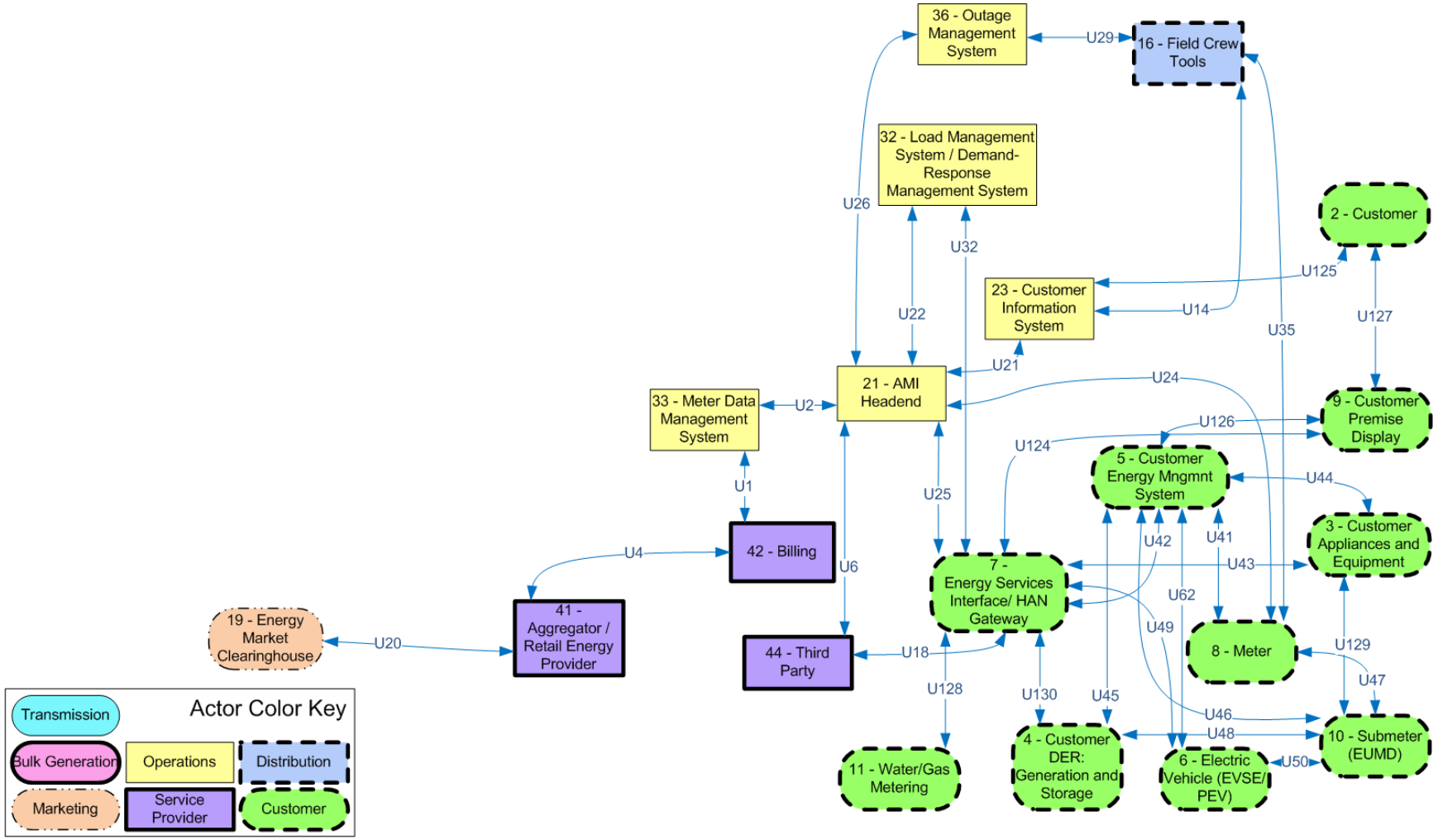

Figure F-5 Customer Premises

Table F-5 Customer Premises by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. 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
2. 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	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. 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	
5. 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
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	none
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U22, U26
8. 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
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U4, U20
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	None
11. 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
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U25, U32, U130
14. 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	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • 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
16. 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, U125
17. 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
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41, U46, U47, U48, U50, U128, U129
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. 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
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. 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

F.6 WIDE AREA SITUATIONAL AWARENESS

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 F-6 shows the diagram for the WASA logical interfaces and associated Table F-6 lists the logical interfaces by category.

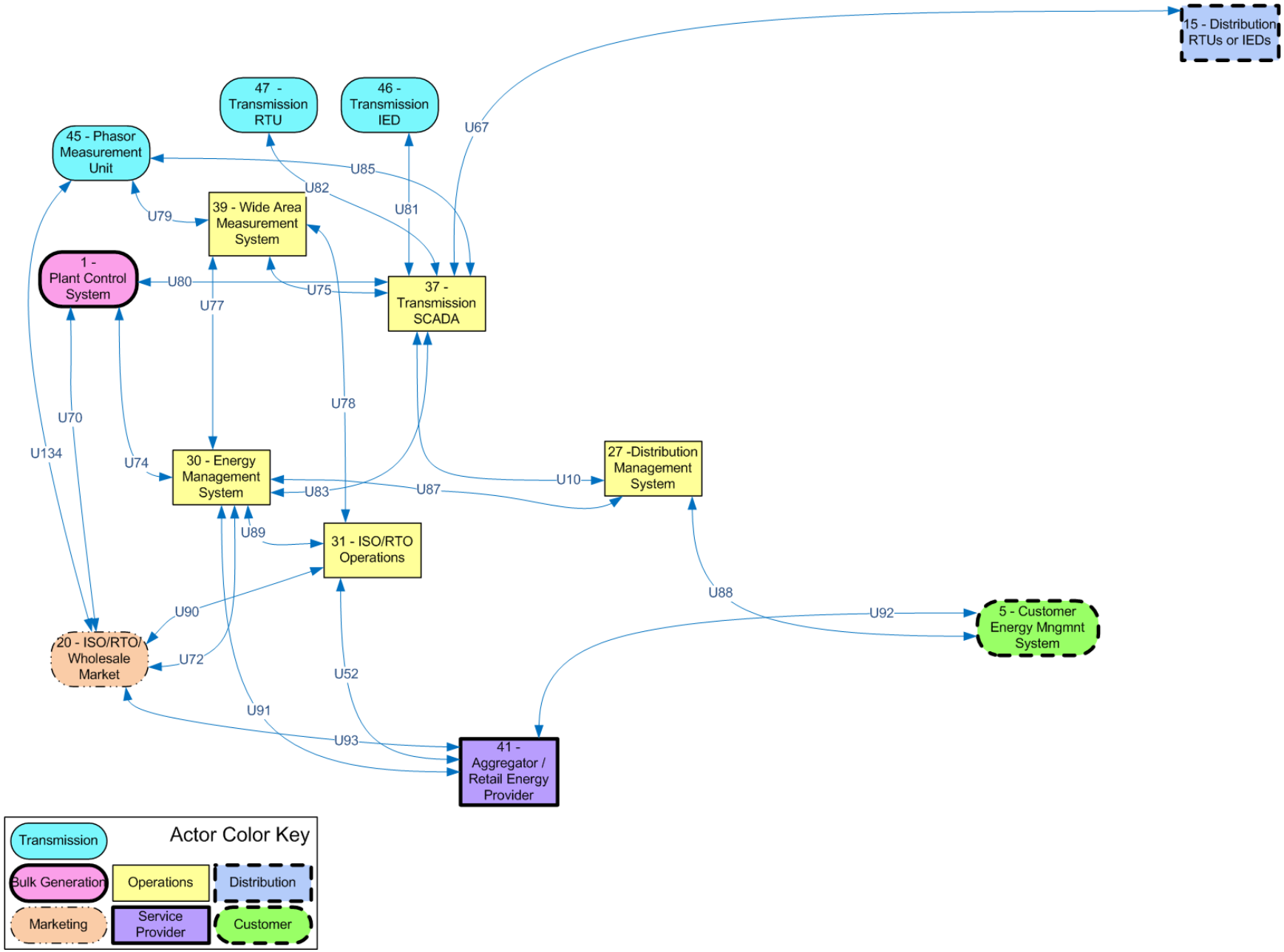

Figure F-6 Wide Area Situational Awareness

Table F-6 WASA Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. 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
2. 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	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. 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	
5. 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
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U10, U74, U80, U83, U87
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	None
8. 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
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U72, U93
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U75, U91
11. 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

Logical Interface Category	Logical Interfaces
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	None
14. 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	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	None
16. 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
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	None
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	U77, U78
20. 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
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. 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

APPENDIX G:
ANALYSIS MATRIX OF LOGICAL 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.

This analysis was one of the tools that was used in the determination of the CI&A impact levels for each logical interface category and in the selection of security requirements. The attribute table was used as a guide for selecting unique technical requirements and determining the impact level for confidentiality, integrity, and availability. The set of attributes allocated to each logical interface category is not intended to be a comprehensive set, or to exclude interfaces that do not include that attribute. For example, a Smart Grid information system may include logical interface category 1, but not ATR-11, legacy information protocols. The goal was to define typical attributes for each logical interface category.

Table G-1 provides additional descriptions of each attribute.

Table G-1 Interface Attributes and Descriptions

Interface Attributes	Descriptions
ATR-1a: Confidentiality requirements	Strong requirement that information should not be viewed by unauthorized entities
ATR-1b: Privacy concerns	Strong requirement that information should not be viewed by unauthorized entities
ATR-2: Integrity requirements	Strong requirement that information should not be modified by unauthorized entities, and should be validated for accuracy and errors. Higher level integrity may require additional technical controls.
ATR-3: Availability requirements	Strong requirement that information should be available within appropriate time frames. Often this necessitates redundancy of equipment, communication paths, and or information sources.
ATR-4: Low bandwidth of communications channels	Severely-limited bandwidth may constrain the types of security technologies that should be used across an interface while still meeting that interface's performance requirements.
ATR-5: Microprocessor constraints on memory and compute capabilities	Severely-limited memory and/or compute capabilities of a microprocessor-based platform may constrain the types of security technologies, such as cryptography, that may be used while still allowing the platform to meet its performance requirements.
ATR-6: Wireless media	Wireless media may necessitate specific types of security technologies to address wireless vulnerabilities across the wireless path.
ATR-7: Immature or proprietary protocols	Immature or proprietary protocols may not be adequately tested either against inadvertent compromises or deliberate attacks. This may leave the interface with more vulnerabilities than if a more mature protocol were used.

Interface Attributes	Descriptions
ATR-8: Inter-organizational interactions	Interactions which cross organizational domains, including the use of out-sourced services and leased networks, can limit trust and compatibility of security policies and technologies. Therefore, these vulnerabilities should be taken into account.
ATR-9: Real-time operational requirements with low tolerance for latency problems	Real-time interactions may entail short acceptable time latencies, and may limit the security technology choices for mitigating on-going attacks.
ATR-11: Legacy communication	Older communication technologies may limit the types, thoroughness, or effectiveness of different security technologies which may be employed. This sensitivity to security technologies should be taken into account.
ATR-10: Legacy end-devices and systems protocols	Older end-devices and protocols may constrain the types, thoroughness, or effectiveness of different security technologies which may be employed.
ATR-12: Insecure, untrusted locations	Devices or systems in locations which cannot be made more secure due to their physical environment or ownership, pose additional security challenges. For instance, hardware-based cryptography may be necessary.
ATR-13: Key management for large numbers of devices	Key management for large numbers of devices without direct access to certificate management may limit the methods for deploying, updating, and revoking cryptographic keys.
ATR-14: Patch and update management constraints for devices including scalability and communications	Patch management constraints may limit the frequency and processes used for updating security patches.
ATR-15: Unpredictability, variability, or diversity of interactions	Unpredictable interactions may complicate the decisions on the types and severity of security threats and their potential impacts
ATR-16: Environmental and physical access constraints	Access constraints may limit the types of security technologies that could be deployed. For instance, if appliances are in a customer's house, access could be very limited.
ATR-17 Limited power source for primary power	Devices with limited power, such as battery-run appliances which "go to sleep" between activities, may constrain the types of security technologies to those that do not require continuous power.
ATR-18: Autonomous control	Autonomous control of devices that may not be centrally monitored could lead to undetected security threats.

Table G-2 provides the analysis matrix of the security-related logical interface categories (rows) against the attributes (ATR) that reflect the interface categories (columns).

Table G-2 Analysis Matrix of Security-Related Logical Interface Categories, Defined by Attributes

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
1. 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
2. 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

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
3. 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
4. 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
5. Interface between control systems within the same organization			X	X						X		X			X				X
6. Interface between control systems in different organizations			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
7. Interface between back office systems under common management authority	X	X	X												X				
8. Interface between back office systems not under common management authority	X	X	X						X						X				
9. Interface with B2B connections between systems usually involving financial or market transactions	X	X	X	X					X	X						X			
10. Interface between control systems and non-control/ corporate systems	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
11. 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	
12. Interface between sensor networks and control systems			X		X	X	X	X		X	X	X		X			X	X	X
13. Interface between systems that use the AMI network	X	X	X		X	X	X	X	X				X	X	X	X	X		
14. 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		

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
15. 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
16. Interface between external systems and the customer site	X	X	X			X		X	X				X	X		X			
17. Interface between systems and mobile field crew laptops/equip-ment			X	X	X		X	X					X	X	X		X		
18. Interface between metering equipment	X	X	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
19. Interface between operations decision support systems			X	X					X	X									
20. Interface between engineering/ maintenance systems and control equipment			X		X	X					X	X	X	X	X		X		
21. Interface between control systems and their vendors for standard maintenance and service			X						X				X	X	X		X		
22. Interface between security/network/ system management consoles and all networks and systems	X	X	X	X						X	X	X		X	X	X	X		

APPENDIX H:
MAPPINGS TO THE HIGH-LEVEL REQUIREMENTS

H.1 R&D TOPICS

The following table is a mapping of research and development topics [See §8] to the High-Level Security Requirements Families.

		Smart Grid Security Requirements Families																
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Device Level	Improve Cost - Effective Higher Tamper Resistant & Survivable Device Architectures					X		X										X		
	Intrusion Detection with Embedded Processors			X				X					X			X				
Novel Mechanisms	Topics in Cryptographic Key Management			X			X			X							X	X		

		Smart Grid Security Requirements Families																		
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Detecting Anomalous Behavior Using Modeling												X		X	X				
System Level	Architecting for bounded recovery and reaction					X		X					X			X				X
	Architecting Real-time security	X					X								X		X	X		
	Calibrating assurance and timeliness trade-offs		X										X		X	X				
	Legacy system integration				X												X		X	X
	Resiliency Management and Decision Support		X	X		X		X					X			X				
	Efficient Composition of Mechanisms																X			

		Smart Grid Security Requirements Families																	
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Risk Assessment and Management																		
Networking	Safe use of COTS/Publicly Available Systems and Networks																X		
	Advanced Networking																X		
	Privacy and Access Control in Federated Systems	X		X			X												
	Auditing and Accountability			X															
	Infrastructure Interdependency Issues																		

		Smart Grid Security Requirements Families																	
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Other Security Issues in the Smart Grid Context	Cross-Domain (Power/Electrical to Cyber/Digital) Security Event Detection, Analysis, and Response					X		X					X			X				
	Network Covert Channels in the Smart Grid: Creation, Characterization, Detection and Elimination					X		X									X			
	DoS/DDoS Resiliency	X				X	X	X									X	X		
	Cloud Security	X					X		X	X							X			
	Security Design & Verification Tools (SD&VT)				X															X

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

H.2 VULNERABILITY CLASSES

The following is a mapping of vulnerability classes [See §6] to the High-Level Security Requirements Families.

			Smart Grid Security Requirements Families																	
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
People, Policy and Procedure	Training	Insufficient Trained Personnel		X			X		X							X					
		Inadequate Security Training and Awareness Program		X			X		X							X					
	Policy and Procedure	Insufficient Identity Validation, Background Checks	X					X				X	X			X					X
		Inadequate Security Policy	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
		Inadequate Privacy Policy													X	X					
		Inadequate Patch Management Process	X			X	X	X	X							X			X	X	
		Inadequate Change and Configuration Management				X										X				X	

			Smart Grid Security Requirements Families																	
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
People, Policy and Procedure		Unnecessary System Access	X			X		X			X	X	X			X					
	Risk Management	Inadequate Periodic Security Audits			X											X					
		Inadequate Security Oversight by Management		X	X							X	X		X	X					
		Inadequate Continuity of Operations or Disaster Recovery Plan					X							X	X	X	X				
		Inadequate Risk Assessment Process														X					
		Inadequate Risk Management Process														X					
		Inadequate Incident Response Process				X			X				X	X		X	X				
		Code Quality Vulnerability		X								X				X		X	X	X	X
		Authentication		X	X			X								X			X	X	X

			Smart Grid Security Requirements Families																
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Platform Software/ Firmware Vulnerabilities	Software Development	Vulnerability																			
		Authorization Vulnerability		X	X			X								X			X	X	X
		Cryptographic Vulnerability		X												X				X	X
		Environmental Vulnerability	X	X				X				X				X		X		X	X
		Error Handling Vulnerability		X												X			X	X	X
		General Logic Error		X												X				X	X
		Input and Output Validation		X												X			X	X	X
		Logging and Auditing Vulnerability		X				X								X				X	X
		Password Management Vulnerability	X	X				X								X				X	X
		Path Vulnerability		X												X				X	X
		Protocol Errors		X												X				X	X

			Smart Grid Security Requirements Families																
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Platform Software/ Firmware Vulnerabilities	Software Development	Range and Type Error Vulnerability		X												X				X	X
		Sensitive Data Protection Vulnerability		X						X						X				X	X
		Session Management Vulnerability		X												X				X	X
		Concurrency, Synchronization and Timing Vulnerability		X												X				X	X
		Insufficient Safeguards for Mobile Code		X												X				X	X
		Buffer Overflow		X												X				X	X
		Mishandling of Undefined, Poorly Defined, or "Illegal" Conditions		X												X				X	X
		Use of Insecure Protocols		X												X		X		X	X
		Weakness that Affect Files and		X												X				X	X

			Smart Grid Security Requirements Families																	
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
		Directories																			
	API Usage & Implementation	API Abuse		X												X				X	X
	API Usage & Implementation	Use of Dangerous API		X												X				X	X
	Design	Inadequate Security Architecture and Design	X	X	X		X	X	X			X		X		X	X	X	X	X	X
Platform Vulnerabilities	Implementation	Inadequate Malware Protection		X	X		X		X					X			X	X	X	X	
Platform Vulnerabilities	Implementation	Installed Security Capabilities Not Enables by Default	X	X	X	X		X						X			X	X	X	X	
Platform Vulnerabilities	Implementation	Absent of Deficient Equipment Implementation Guidelines	X	X	X	X		X						X		X	X	X		X	

			Smart Grid Security Requirements Families																	
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Operational	Lack of Prompt Security Patches from Software Vendors			X		X		X									X	X	X	
		Unneeded Services Running		X	X	X								X			X	X	X	X	
		Insufficient Log Management	X	X	X	X	X	X	X		X			X			X	X	X	X	
		Inadequate Anomaly Tracking	X	X	X		X	X	X			X	X	X			X	X	X	X	
	Network	Inadequate Integrity Checking				X									X			X	X	X	X
		Inadequate Network Segregation				X									X	X			X	X	X
		Inappropriate Protocol Selection				X									X			X	X	X	X
		Weakness in Authentication Process or Authentication Keys				X									X	X		X	X	X	X
		Insufficient Redundancy				X														X	X
		Physical Access to the Device	X			X		X				X	X		X	X					X

BOTTOM-UP TOPICS

The following is a mapping of topics identified in the Bottom-up chapter [See §7] to the High-Level Security Requirements Families.

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Openness and Accessibility of Smart Grid Standards														X					
Authenticating and Authorizing Users to Substation IEDs						X													
Authenticating and Authorizing Users to Outdoor Field Equipment						X													
Authenticating and Authorizing Maintenance Personnel to Meters						X													
Authenticating and Authorizing Consumers to Meters						X													
Authenticating Meters to/from AMI Head Ends						X													
Authenticating HAN Devices to/from HAN Gateways						X													

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authenticating Meters to/from AMI Networks						X													
Securing Serial SCADA Communications																X			
Securing Engineering Dial-up Access																X			
Secure End-to-End Meter to Head End Communication																X			
Access Logs for IEDs			X																
Remote Attestation of Meters																X	X		X
Protection of Routing Protocols in AMI Layer 2/3 Networks																X	X		
Key Management for Meters																X			
Protection of Dial-up Meters																X			
Outsourced WAN Links																X			
Insecure Firmware Updates																	X	X	
Side Channel Attacks on Smart Grid Field Equipment						X										X			
Securing and Validating Field Device Settings	X					X										X			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Absolute & Accurate Time Information			X			X										X			
Security Protocols																			
Synchrophasors																			
Certificates																			
Event Logs and Forensics																			
Personnel Issues In Field Service Of Security Technology																			
Weak Authentication of Devices In Substations						X					X								
Weak Security for Radio-Controlled Distribution Devices						X										X			
Weak Protocol Stack Implementations																X			
Insecure Protocols																			
License Enforcement Functions																			
IT vs. Smart Grid Security																			
Patch Management																	X		

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authentication	X			X		X													
System Trust Model																X			
User Trust Model																X			
Security Levels																			
Distributed vs. Centralized Model of Management																			
Local Autonomy of Operation																			
Intrusion Detection for Power Equipment				X		X											X		
Network and System and Management for Power Equipment	X			X		X											X		
Security Event Management					X		X										X		X
Cross-Utility / Cross-Corporate Security																			
Trust Management																			
Management of Decentralized Security Controls																			
Password Management	X					X													
Cipher Suite																X			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authenticating Users to Control Center Devices and Services						X													
Authentication of Devices to Users						X													
Entropy																			
Tamper Evidence	X										X					X			
Challenges with Securing Serial Communications																			
Legacy Equipment with Limited Resources																X		X	X
Costs of Patch and Applying Firmware Updates	X	X		X		X					X						X		
Forensics and Related Investigations			X		X		X										X		
Roles and Role Based Access Control	X					X													
Limited Sharing of Vulnerability and/or Incident Information														X					
Data Flow Control Vulnerability Issues																			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Use of Shared/Dedicated and Public/Private Cyber Resources																			
Traffic Analysis						X										X	X		
Poor Software Engineering Practices																	X		
Attribution of Faults to the Security System																			
Need for Unified Requirements Model																			
Broad Definition of Availability																			
Utility Purchasing Practices																		X	
Cyber Security Governance																			
Key Management Issues																			
Summarized Issues with PKI																			
Key Management Systems for Smart Grid																X			
Computational Constraints																			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Channel Bandwidth																			
Connectivity																			
Certificate Life Cycles																X			
Local Autonomy of Operation																			
Availability																			
Trust Roots																			
Algorithms and Key Lengths																			
Selection and Use of Cryptographic Techniques																X			
Elliptic Curve Cryptography (ECC)														X					
Break Glass Authentication																			
Cryptographic Module Upgradeability																			
Password Complexity Rules	X					X													
Authentication						X													
Network Access Authentication and Access Control	X					X													

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Random Number Generation & Entropy																			
Single Sign On (SSO)																			

APPENDIX I:
GLOSSARY AND ACRONYMS

3DES	Triple Data Encryption Standard (168 Bit)
AAA	Authentication, Authorization, and Accounting
Active Directory	A technology created by Microsoft that provides a variety of network services and is a central component of the Windows Server platform. The directory service provides the means to manage the identities and relationships that make up network environments.
ADA	Americans with Disabilities Act
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AGA	American Gas Association
AGC	Automatic Generation Control. A standalone subsystem that regulates the power output of electric generators within a prescribed area in response to changes in system frequency, tie-line loading, and the relation of these to each other. This maintains the scheduled system frequency and established interchange with other areas within predetermined limits.
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
AMI-SEC	AMI Security [Task Force]
Anonymize	• To organize data in such a way as to preserve the anonymity or hide the personal identity of the individual(s) to whom the data pertains • A process of transformation or elimination of PII for purposes of sharing data
ANSI	American National Standards Institute
API	Application Programming Interface
ASAP-SG	Advanced Security Acceleration Project – Smart Grid
ASTM	American Society for Testing and Materials
Asymmetric cipher	Cryptography solution in which separate keys are used for encryption and decryption, where one key is public and the other is private.
ATR	Attribute
B2B	Business to Business
BAN	Building Area Network
BEM	Building Energy Management

Block cipher	A symmetric key cipher operating on fixed-length groups of bits, called blocks, with an unvarying transformation—in contrast to a stream cipher, which operates on individual digits one at a time and whose transformation varies during the encryption. A block cipher, however, can effectively act as a stream cipher when used in certain modes of operation.
Botnet	Robot Network. A large number of compromised computers also called a "zombie army," that can be used to flood a network with messages as a denial of service attack. A thriving botnet business consists in selling lists of compromised computers to hackers and spammers.
C&I	Commercial and Industrial
CA	Certificate Authority
CALEA	Communications Assistance for Law Enforcement Act
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
CBC	Cipher Block Chaining
CEC	California Energy Commission
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CHP	Combined Heat and Power
CI&A	Confidentiality, Integrity, and Availability
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.
CIMA	Chartered Institute of Management Accountants
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPA	Children's Internet Protection Act
CIS	Cryptographic Interoperability Strategy
CIS	Customer Information System
CISO	Chief Information Security Officer
CMMS	Computer-based Maintenance Management Systems
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSCTG	Cyber Security Coordination Task Group
CSO	Chief Security Officer
CSP	Critical Security Parameters
CSR	Certificate Signing Request

CSR	Customer Service Representative
CSSWG	Control Systems Security Working Group
CSWG	Cyber Security Working Group
CRT	Cathode Ray Tube
CTR mode	Counter mode. A block cipher mode of operation also known as Integer Counter Mode (ICM) and Segmented Integer Counter (SIC) mode.
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DA	Distribution Automation
DARPA	Defense Advanced Research Projects Agency
DCS	Distributed Control System. A computer-based control system where several sections within the plants have their own processors, linked together to provide both information dissemination and manufacturing coordination.
DDoS	Distributed Denial of Service
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
DES	Data Encryption Standard
DEWG	Domain Expert Working Group
DFR	Digital Fault Recorder
DGM	Distribution Grid Management
DHS	Department of Homeland Security
Diffie-Hellman	A cryptographic key exchange protocol first published by Whitfield Diffie and Martin Hellman in 1976. It allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
Distinguished names	String representations that uniquely identify users, systems, and organizations.
DMS	Distribution Management System
DN	Distinguished Name
DNP	Distributed Network Protocol
DNS	Domain Name Service
DoD	Department of Defense
DOE	Department of Energy
DoS	Denial of Service
DR	Demand Response
DRBG	Deterministic Random Bit Generators

DRM	Digital Rights Management. A generic term for access control technologies used by standards providers, publishers, copyright holders, manufacturers, etc. to impose limitations on the usage of digital content and devices. The term is used to describe any technology that inhibits the use of digital content in a manner not desired or intended by the content provider.
DRMS	Distribution Resource Management System
DSL	Digital Subscriber Line
DSPF	Distribution System Power Flow
DSS	Digital Signature Standard
EAP	Extensible Authentication Protocol
EAX mode	• A mode of operation for cryptographic block ciphers. It is an AEAD algorithm designed to simultaneously provide both authentication and privacy of the message with a two-pass scheme, one pass for achieving privacy and one for authenticity for each block. • A mixed authenticated encryption mode of operation of a block cipher in order to reduce the area overhead required by traditional authentication schemes.
EAX'	A modification of the EAX mode used in the ANSI C12.22 standard for transport of meter-based data over a network.
ECC	Elliptic Curve Cryptography (encryption)
ECDH	Elliptic Curve Diffie-Hellman. A key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel.
ECDSA	Elliptic Curve Digital Signature Algorithm
ECPA	Electronic Communications Privacy Act
EEO	Equal Employment Opportunity
EEPROM	Electrically Erasable Programmable Read-Only Memory
EISA	Energy Independence and Security Act
EKU	Extended Key Usage
EMS	Energy Management System
EMSK	Extended Master Session Key
Entropy	In the case of transmitted messages, a measure of the amount of information that is missing before reception.
Ephemeral Unified Model	A ECDH scheme where each party generates an ephemeral key pair to be used in the computation of the shared secret.
EPIC	Electronic Privacy Information Center
EPRI	Electric Power Research Institute
EPSA	Electric Power Supply Association
ES	Electric Storage
ESI	Energy Services Interface

ESP	Energy Service Provider
ET	Electric Transportation
EUMD	End Use Measurement Device
EV	Electric Vehicle
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.
EvDO	Evolution Data Optimized
EVSE	Electric Vehicle Service Element
FACTA	Fair and Accurate Credit Transactions Act
FAQ	Frequently Asked Questions
FERC	Federal Energy Regulatory Commission
FERPA	Family Educational Rights and Privacy Act
FIPS	Federal Information Processing Standards
FIPS 140-2	Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules. NIST issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components.
FLIR	Fault Location, Isolation, Restoration
FTP	File Transfer Protocol
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.
GIC	Group Insurance Commission
GIS	Geographic Information System
GLBA	Gramm-Leach Bliley Act
GPRS	General Packet Radio Service
GPSK	Generalized Pre-Shared Key
Granularity	The extent to which a system contains separate components, e.g., the fineness or coarseness with which data fields are subdivided in data collection, transmission, and storage systems. The more components in a system, the more flexible it is. In more general terms, the degree to which a volume of information is finely detailed.
GRC	Governance, Risk, and Compliance
GWAC	GridWise Architecture Council

Hacker	In common usage, a hacker is a person who breaks into computers and/or computer networks, usually by gaining access to administrative controls. Proponents may be motivated by diverse objectives from the shear entertainment value they find in the challenge of circumventing computer/network security to political or other ends. Hackers are often unconcerned about the use of illegal means to achieve their ends. Out-and-out cyber-criminal hackers are often referred to as "crackers."
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.
Hash	Any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array. The values returned by a hash function are called hash values, hash codes, hash sums, checksums, or simply hashes.
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hz	hertz
IBE	Identity-Based Encryption
ICS	Industrial Control Systems
ID	Identification
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFAC	International Federation of Accountants
IKE	Internet Key Exchange. Protocol used to set up a security association in the IPsec protocol suite.
INL	Idaho National Laboratory
IP	Internet Protocol
IPP	Independent Power Producer
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System

IPSec	Internet Protocol Security
IS	Information Security
ISA	International Society of Automation
ISAKMP	Internet Security Association and Key Management Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
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
ITGI	IT Governance Institute
ITL	Information Technology Laboratory
IVR	Interactive Voice Response
JNI	Java Native Interface
JTC	Joint Technical Committee
KDC	Key Distribution Center
KEK	Key Encryption Key
Kerberos	A computer network authentication protocol, developed by the Massachusetts Institute of Technology, which allows nodes communicating over a nonsecure network to prove their identity to one another in a secure manner. It is also a suite of free software published by MIT that implements this protocol.
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LMS	Load Management System
LTC	Load Tap Changer
MAC	Message Authentication Code
MAC address	Media Access Control address. The unique serial number burned into Ethernet and Token Ring adapters that identifies that network card from all others.
MAC protection	Message Authentication Code protection. In cryptography, a short piece of information used to authenticate a message. The MAC value protects data integrity and authenticity of the tagged message by allowing verifiers (who also possess the secret key used to generate the value) to detect any changes to the message content.
MDMS	Meter Data Management System

min	minute
MIT	Massachusetts Institute of Technology
MITM	Man in the Middle
ms	millisecond (10^{-3} second)
MTBF	Mean Time Before Failure
MW	megawatt (10^{6} watts)
NAN	Neighborhood Area Network
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NMAP	Networked Messaging Application Protocol
NRECA	National Rural Electric Cooperative Association
NSA	National Security Agency
NSA Suite B	A set of cryptographic algorithms promulgated by the National Security Agency to serve as an interoperable cryptographic base for both unclassified information and most classified information.
NSF	National Science Foundation
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OE	Office of Electricity Delivery and Energy Reliability
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.
OID	Object Identifier
OMS	Outage Management System
One-Pass Diffie-Hellman	A key-agreement scheme in which an ephemeral key pair generated by one party is used together with the other party's static key pair in the computation of the shared secret.
OWASP	Open Web Application Security Project
PANA	Protocol for carrying Authentication for Network Access
PAP	Priority Action Plan
PC	Personal Computer
PDA	Personal Digital Assistant
PDC	Phasor Data Concentrator

PE	Protocol Encryption
PE mode	• An encryption mode combining CTR mode and ECB mode developed for streaming SCADA messages. It relies on the SCADA protocol's ability to detect incorrect SCADA messages. • Position Embedding mode. A cryptographic mode designed specifically for low latency integrity protection on low-speed serial links.
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
PFS	Perfect Forward Secrecy
PHEV	Plug In Hybrid Electric Vehicle
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 Identifiable Information
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKMv2	Privacy Key Management version 2
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PQ	Power Quality
Public-key cryptography	A cryptographic approach that involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver.
PUC	Public Utilities Commission
QoS	Quality of Service
R&D	Research and Development
RA	Registration Authority
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RBAC	Role-Based Access Control

Retail Access	Competitive retail or market-based pricing offered by energy services companies or utilities to some or all of their customers under the approval/regulation of state public utilities departments.
RF	Radio Frequency
RFC	Request for Comments
RNG	Random Number Generator
RP	Relying Party
RSA	Widely used in electronic commerce protocols, this algorithm for public-key cryptography is named for Rivest, Shamir, and Adleman who were first to publicly described it. This was the first algorithm known to be suitable for signing as well as encryption and represents a great advance in public key cryptography.
RSA algorithm	RSA is public key cryptography algorithm named for its co-inventors: Ron Rivest, Adi Shamir, and Len Adleman.
RTO	Regional Transmission Operator
RTP	Real-Time Pricing
RTU	Remote Terminal Unit
s	second
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	Security Association
SAM	Security Authentication Module
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDLC	Software Development Life Cycle
SDO	Standard Developing Organization
SEL	Schweitzer Engineering Laboratories
SEM	Security Event Management
SEP	Smart Energy Profile
SGIP	Smart Grid Interoperability Panel
SGIP TWiki	An open collaboration site for the Smart Grid community to work with NIST in developing a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems and is part of a robust process for continued development and implementation of standards as needs and opportunities arise and as technology advances.
SGIP-CSWG	SGIP – Cyber Security Working Group
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

Single sign-on	A property of access control of multiple, related, but independent software systems. With this property a user/device logs in once and gains access to all related systems without being prompted to log in again at each of them.
SNMP	Simple Network Management Protocol
Social Engineering	The act of manipulating people into performing actions or divulging confidential information. The term typically applies to trickery or deception being used for purposes of information gathering, fraud, or computer system access.
SP	Special Publication
SPOF	Signal Point of Failure
SSH	Secure Shell. A protocol for secure remote login and other secure network services over an insecure network.
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSL/TLS	Secure Socket Layer / Transport Layer Security
SSN	Social Security Number
SSO	Single Sign-On
SSP	Sector-specific Plans
Symmetric cipher	Cryptography solution in which both parties use the same key for encryption and decryption, hence the encryption key must be shared between the two parties before any messages can be decrypted.
T&D	Transmission and Distribution
T&D DEWG	T&D Domain Expert Working Group
TA	Trust Anchor
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TCPA	Telephone Consumer Protection Act
TCS	Trouble Call System
Telnet	Teletype network. A network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility. The term telnet may also refer to the software that implements the client part of the protocol.
TEMPEST	A codename referring to investigations and studies of conducted emissions. Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.
TLS	Transport Layer Security
TNC	Trusted Network Connect
TOCTOU	Time of Check, Time of Use

TPI	Two-Person Integrity
TRSM	Tamper Resistant Security Modules
Trust anchor	In cryptography, an authoritative entity represented via a public key and associated data. When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor. The public key (of the trust anchor) is used to verify digital signatures and the associated data.
TWiki	A flexible, open source collaboration and Web application platform (i.e., a structured Wiki) typically used to run a project development space, a document management system, a knowledge base, or any other groupware tool on an intranet, extranet, or the Internet to foster information flow between members of a distributed work group.
UCAIug	UtiliSec Working Group
UDP/IP	User Datagram Protocol/Internet Protocol
Upsell	Marketing term for the practice of suggesting higher priced products or services to a customer who is considering a purchase.
URL	Universal Resource Locator
USRK	Usage-Specific Root Key
Van Eck phreaking	Named after Dutch computer researcher Wim van Eck, phreaking is the process of eavesdropping on the contents of a CRT and LCD display by detecting its electromagnetic emissions. Because of its connection to eavesdropping, the term is also applied to exploiting telephone networks.
VAR	Volts-Amps-Reactive
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAMS	Wide Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WG	Working Group
Wi-Fi	Term often used as a synonym for IEEE 802.11 technology. Wi-Fi is a trademark of the Wi-Fi Alliance that may be used with certified products that belong to a class of WLAN devices based on the IEEE 802.11 standards.
WiMAX	• Worldwide Interoperability for Microwave Access. A telecommunications protocol that provides fixed and fully mobile Internet access. • Wireless digital communications system, also known as IEEE 802.16, which is intended for wireless "metropolitan area networks."
WLAN	Wireless Local Area Network
WMS	Work Management System
XML	Extensible Markup Language

APPENDIX J:
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 subgroups.

	Name	Organization
1.	Aber, Lee	OPOWER
2.	Ackerman, Eric	Edison Electric Institute
3.	Akyol, Bora	Pacific Northwest National Laboratory
4.	Alexander, Roger	Eka Systems, Inc.
5.	Alrich, Tom	ENCARI
6.	Ambady, Balu	Sensus
7.	Anderson, Dwight	Schweitzer Engineering Labs
8.	Arneja, Vince	Arxan Technologies, Inc.
9.	Ascough, Jessica	Harris Corporation
10.	Bacik, Sandy	Enernex
11.	Baiba Grazdina	Duke Energy
12.	Baker, Fred	Cisco Systems, Inc.
13.	Balsam, John	Georgia Tech Research Institute
14.	Barber, Mitch	Industrial Defender, Inc.
15.	Barclay, Steve	ATIS
16.	Barnes, Frank	University of Colorado at Boulder
17.	Barnett, Bruce	GE Global Research
18.	Barr, Michael	L-3 Communications Nova Engineering
19.	Bass, Len	Software Engineering Institute Carnegie Mellon University
20.	Basu, Sourjo	General Electric Energy
21.	Batz, David	Edison Electric Institute
22.	Bell, Ray	Grid Net
23.	Bell, Will	Grid Net
24.	Bemmel, Vincent	Trilliant
25.	Bender, Klaus	Utilities Telecom Council
26.	Benn, Jason	Hawaiian Electric Company
27.	Berkowitz, Don	S&C Electric Company
28.	Beroset, Ed	Elster Group
29.	Berrett, Dan E.	DHS Standards Awareness Team (SAT)
30.	Berrey, Adam	General Catalyst Partners
31.	Bertholet, Pierre-Yves	Ashlawn Energy, LLC
32.	Beyene, Tsegereda	Cisco Systems, Inc.
33.	Bhaskar, Mithun M.	National Institute of Technology, Warangal
34.	Biggs, Doug	Infogard
35.	Biggs, Les	Infogard

	Name	Organization
36.	Blomgren, Paul	SafeNet Inc.
37.	Bobba, Rakesh	University of Illinois, Urbana-Champaign
38.	Bochman, Andy	
39.	Boivie, Rick	IBM T. J. Watson Research Center
40.	Bradley, Steven	Virginia State Corporation Commission
41.	Braendle, Markus	ABB
42.	Branco, Carlos	Northeast Utilities
43.	Brenton, Jim	Ercot
44.	Brewer, Tanya	NIST
45.	Brigati, David	NitroSecurity
46.	Brinskele, Ed	Vir2us Inc.
47.	Brooks, Thurston	3e Technologies International, Inc.
48.	Brown, Bobby	Consumers Energy / EnerNex Corporation
49.	Brozek, Mike	Westar Energy, Inc.
50.	Bryan, Clifford	Examiner.com
51.	Bucciero, Joe	Buccerio Consulting
52.	Burnham, Laurie	Dartmouth College
53.	Butterworth, Jim	Guidance Software
54.	Camilleri, John	Green Energy Corp
55.	Campagna, Matt	Certicom Corp.
56.	Cam-Winget, Nancy	Cisco Systems, Inc.
57.	Caprio, Daniel	McKenna Long & Aldridge LLP
58.	Cardenas, Alvaro A.	Fujitsu
59.	Carlson, Chris	Puget Sound Energy
60.	Carpenter, Matthew	Consumers Energy / InGuardians
61.	Chaney, Mike	Securicon
62.	Chasko, Stephen	Landis+Gyr
63.	Choubey, T. N.	
64.	Chow, Edward	U of Colorado at Colorado Springs
65.	Chris Starr	General Dynamics
66.	Christopher, Jason	FERC
67.	Chudgar, Raj	Sungard
68.	Cioni, Mark V.	MV Cioni Associates, Inc.
69.	Claypoole, Ted	Womble Carlyle Sandridge & Rice, PLLC
70.	Clements, Sam	Pacific Northwest National Laboratory
71.	Cleveland, Frances	Xanthus Consulting International
72.	Cohen, Mike	Mitre
73.	Collier, Albert	Alterium, LLC
74.	Coney, Lillie	Electronic Privacy Information Center
75.	Coomer, Mark	ITT Defense and Information Solutions
76.	Coop, Mike	heyCoop, LLC
77.	Cornish, Kevin	Enspiria
78.	Cortes, Sarah	Inman Technology IT

	Name	Organization
79.	Cosio, George	Florida Power and Light
80.	Cragie, Robert	Jennic LTD
81.	Crane, Melissa	Tennessee Valley Authority
82.	Cui, Stephen	Microchip Technology
83.	Dagle, Jeff	Pacific Northwest National Laboratory
84.	Dalva, Dave	Cisco Systems, Inc.
85.	Danahy, Jack	Bochman & Danahy Research
86.	Dangler, Jack	SAIC
87.	Davis, Scott	Sensus
88.	De Petrillo, Nick	Industrial Defender
89.	Delenela, Ann	Ercot
90.	DeLoach, Tim	IBM Global Business Services
91.	di Sabato, Mark	
92.	Dillon, Terry	APS
93.	Dinges, Sharon	Trane
94.	Dion, Thomas	Dept of Homeland Security
95.	Dodd, David	pbnetworks
96.	Dodson, Greg	Dominion Resources Services, Inc.
97.	Don-Arthur, George	Alterium LLC
98.	Doreswamy, Rangan	Verisign, Inc.
99.	Dorn, John	Accenture
100.	Dougherty, Steven	IBM
101.	Downum, Wesley	Telcordia
102.	Dransfield, Michael	National Security Agency
103.	Drozinski, Timothy	Florida Power & Light Company
104.	Drummond, Rik	Drummond Group
105.	Dubrawsky, Ido	Itron
106.	Duggan, Pat	ConEd
107.	Dulaney, Mike	Arxan Technologies, Inc.
108.	Dunfee, Rhonda	Department of Energy
109.	Dunton, Benjamin	NYS Department of Public Service
110.	Dupper, Jeff	Ball Aerospace & Technologies
111.	Duren, Michael	Protected Computing
112.	Dutta, Prosenjit	Utilities AMI Practice
113.	Earl, Frank	Earl Consulting
114.	Eastham, Bryant	Panasonic Electric Works Laboratory of America (PEWLA)
115.	Edgar, Tom	Pacific Northwest National Laboratory
116.	Eggers, Matthew	U.S. Chamber of Commerce
117.	Eigenhuis, Scott M	
118.	Emelko, Glenn	ESCO
119.	Engels, Mark	Dominion Resources Services, Inc.
120.	Ennis, Greg	Wi-Fi Alliance

	Name	Organization
121.	Enstrom, Mark	NeuStar
122.	Eraker, Liz	Samuelson Clinic at UC Berkeley
123.	Estefania, Maria	ATIS
124.	Eswarahally, Shrinath	Infineon Technologies NA
125.	Ewing, Chris	Schweitzer Engineering Labs
126.	Fabela, Ronnie	Lockheed Martin
127.	Faith, Doug	MW Consulting
128.	Faith, Nathan	American Electric Power
129.	Famolari, David	Telcordia Technologies
130.	Fennell, Kevin	Landis+Gyr
131.	Fischer, Ted	Norwich University Applied Research Institutes (NUARI)
132.	Fisher, Jim	Noblis
133.	Fishman, Aryah	Edison Electric Institute
134.	Franz, Matthew	SAIC
135.	Fredebeil, Karlton	Tennessee Valley Authority
136.	Freund, Mark	Pacific Gas and Electric Company
137.	Frogner, Bjorn	
138.	Fulford, Ed	
139.	Fuloria, Shailendra	Cambridge University
140.	Fulton, Joel	
141.	Gailey, Mike	CSC
142.	Garrard, Ken	Aunigma Network Solutions Corp.
143.	Gerber, Josh	San Diego Gas and Electric
144.	Gerbino, Nick	Dominion Resources Services, Inc.
145.	Gering, Kip	Itron
146.	Gerra, Arun	University of Colorado, Boulder
147.	Ghansah, Isaac	California State University Sacramento
148.	Gibbs, Derek	SmartSynch
149.	Gillmore, Matt	CMS Energy
150.	Givens, Beth	Privacy Rights Clearinghouse
151.	Glenn, Bill	Westar Energy, Inc.
152.	Goff, Ed	Progress Energy
153.	Golla, Ramprasad	Grid Net
154.	Gonzalez, Efrain	Southern California Edison
155.	Gooding, Jeff	Southern California Edison
156.	Goodson, Paul	ISA
157.	Gorog, Christopher	Atmel Corporation
158.	Grainger, Steven	General Dynamics
159.	Grazdina, Baiba	Duke Energy
160.	Greenberg, Alan M.	Boeing
161.	Greenfield, Neil	American Electric Power, Inc.
162.	Greer, David	University of Tulsa
163.	Griffin, Slade	Enernex

	Name	Organization
164.	Grochow, Jerrold	MIT
165.	Gulick, Jessica	SAIC
166.	Gunter, Carl	U. of Illinois
167.	Gupta, Rajesh	UC San Diego
168.	Gupta, Sarbari	Electrosoft
169.	Habre, Alex	PJM
170.	Hague, David	
171.	Halasz, Dave	Aclara
172.	Halbgewachs, Ronald D.	Sandia National Laboratories
173.	Hall, Tim	Mocana
174.	Hallman, Georgia	Guidance Software
175.	Hambrick, Gene	Carnegie Mellon University
176.	Hardjono, Thomas	MIT
177.	Hawk, Carol	Department of Energy
178.	Hayden, Ernest	Verizon
179.	He, Donya	BAE Systems
180.	Heiden, Rick	Pitney Bowes
181.	Hensel, Hank	CSC
182.	Herold, Rebecca	Privacy Professor Rebecca Herold & Associates, LLC
183.	Heron, George L.	BlueFin Security
184.	Herrell, Jonas	University of California, Berkeley
185.	Hertzog, Christine	Smart Grid Library
186.	Highfill, Darren	SCE
187.	Hilber, Del	Constellation Energy
188.	Histed, Jonathan	Novar | Honeywell
189.	Hoag, John C.	Ohio University
190.	Holstein, Dennis	OPUS Consulting Group
191.	Hoofnagle, Chris	University of California, Berkeley
192.	House, Joshua	Future of Privacy
193.	Houseman, Doug	Capgemini Consulting
194.	Huber, Robert	Critical Intelligence
195.	Hughes, Joe	EPRI
196.	Hunteman, William	Department of Energy
197.	Hurley, Jesse	Shift Research, LLC
198.	Hussey, Laura	Schweitzer Engineering Laboratories, Inc.
199.	Hutson, Jeff	Accenture
200.	Huzmezan, Mihai	General Electric
201.	Ibrahim, Erfan	EPRI
202.	Iga, Yoichi	Renesas Electronics Corp.
203.	Ilic, Marija	Carnegie-Mellon University
204.	Iorga, Michaela	NIST
205.	Ivers, James	SEI
206.	Jacobs, Leonard	Xcel Energy

	Name	Organization
207.	Jaokar, Ajit	Futuretext
208.	Jeirath, Nakul	Southwest Research Institute
209.	Jepson, Robert	Lockheed Martin Energy Solutions
210.	Jin, Chunlian	Pacific Northwest National Laboratory
211.	Joffe, Rodney	NeuStar
212.	Johnson, Freemon	NIST
213.	Johnson, Oliver	Tendril
214.	Jones, Barry	Sempra
215.	Jones, Derrick	Enteredge Technology, LLC
216.	Kahl, Steve	North Dakota
217.	Kalbfleisch, Roderick	Northeast Utilities
218.	Kanda, Mitsuru	Toshiba
219.	Kashatus, Jennifer	Womble Carlyle Sandridge & Rice, PLLC
220.	Kastner, Ryan	University of California at San Diego
221.	Kellogg, Shannon	EMC
222.	Kenchington, Henry	Department of Energy
223.	Kerber, Jennifer	Tech America
224.	Khurana, Himanshu	University of Illinois
225.	Kiely, Sarah	NRECA
226.	Kim, Jin	Risk Management Consulting, CRA International
227.	Kimura, Randy	General Electric
228.	King, Charlie	BAE Systems
229.	Kirby, Bill	Aunigma Network Solutions Corp.
230.	Kiss, Gabor	Telcordia
231.	Kladko, Stan	Aspect Labs
232.	Klein, Stanley A.	Open Secure Energy Control Systems, LLC
233.	Klerer, Mark	
234.	Kobayashi, Nobuhiro	Mitsubishi Electric
235.	Koliwad, Ajay	General Electric
236.	Kotting, Chris	Ohio PUC
237.	Krishnamurthy, Hema	ITT Information Assurance
238.	Kube, Nate	Wurldtech
239.	Kulkarni, Manoj	Mocana
240.	Kursawe, Klaus	Philips
241.	Kuruganti, Phani Teja	EMC2
242.	Kyle, Martin	Sierra Systems
243.	Lackey, Kevin	Electric Reliability Council of Texas (ERCOT)
244.	Lakshminarayanan, Sitaraman	General Electric
245.	LaMarre, Mike	Austin Energy ITT
246.	Larsen, Harmony	Infogard
247.	Lauriat, Nicholas A.	Network and Security Technologies
248.	LaVoy, Lanse	DTE Energy

	Name	Organization
249.	Lawson, Barry	NRECA
250.	Lee, Annabelle	FERC
251.	Lee, Cheolwon	Electronics and Telecommunications Research Institute
252.	Lee, Gunhee	Electronics and Telecommunications Research Institute
253.	Lee, JJ	LS Industrial Systems
254.	Lee, Virginia	eComp Consultants
255.	Lenane, Brian	SRA International
256.	Leuck, Jason	Lockheed Martin Corporation
257.	Levinson, Alex	Lockheed Martin Information Systems and Global Solutions
258.	Lewis, David	Hydro One
259.	Lewis, Rob	Trustifiers Inc.
260.	Libous, Jim	Lockheed Martin Systems Integration – Owego
261.	Lilley, John	Sempra
262.	Lima, Claudio	Sonoma Innovation
263.	Lintzen, Johannes	Utimaco Safeware AG
264.	Lipson, Howard	CERT, Software Engineering Institute
265.	Lynch, Jennifer	University of California, Berkeley
266.	Maciel, Greg	Uniloc USA
267.	Magda, Wally	Industrial Defender
268.	Magnuson, Gail	
269.	Manjrekar, Madhav	Siemens
270.	Manucharyan, Hovanes	LinkGard Systems
271.	Maria, Art	AT&T
272.	Markham, Tom	Honeywell
273.	Marks, Larry	
274.	Martinez, Catherine	DTE Energy
275.	Martinez, Ralph	BAE Systems
276.	Marty, David	University of California, Berkeley
277.	McBride, Sean	Critical Intelligence
278.	McComber, Robert	Telvent
279.	McCullough, Jeff	Elster Group
280.	McDonald, Jeremy	Southern California Edison
281.	McGinnis, Douglas	IT Utility Solutions
282.	McGrew, David	Cisco
283.	McGurk, Sean	Dept of Homeland Security
284.	McKay, Brian	Booz Allen Hamilton
285.	McKinnon, David	Pacific Northwest National Laboratory
286.	McMahon, Liam	Bridge Energy Group
287.	McQuade, Rae	NAESB
288.	Melton, Ron	Pacific Northwest National Laboratory
289.	Mertz, Michael	Southern California Edison
290.	Metke, Tony	Motorola

	Name	Organization
291.	Milbrand, Doug	Concurrent Technologies Corporation
292.	Millard, David	Georgia Tech Research Institute
293.	Miller, Joel	Merrion Group
294.	Mirza, Wasi	Motorola
295.	Mitsuru, Kanda	Toshiba
296.	Modeste, Ken	Underwriters Laboratories, Inc.
297.	Moise, Avy	Future DOS R&D Inc.
298.	Molina, Jesus	Fujitsu Ltd.
299.	Molitor, Paul	NEMA
300.	Mollenkopf, Jim	CURRENT Group
301.	Moniz, Paulo	Logica
302.	Morris, Tommy	Mississippi State University
303.	Moskowitz, Robert	ICSAlabs
304.	Mulberry, Karen	Neustar
305.	Nahas, John	ICF International
306.	Navid, Nivad	Midwest ISO
307.	Newhouse, Bill	NIST
308.	Nguyen, Nhut	Samsung
309.	Noel, Paul	ASI
310.	Norton, Dave	Entergy
311.	Nutaro, James J.	Southern California Edison
312.	O'Neill, Ivan	Southern California Edison
313.	Ohba, Yoshihiro	Toshiba
314.	Okunami, Peter M.	Hawaiian Electric Company, Inc.
315.	Old, Robert	Siemens Building Technologies, Inc.
316.	Olive, Kay	Olive Strategies
317.	Overman, Thomas M.	Boeing
318.	Owens, Andy	Plexus Research
319.	Pace, James	Silver Spring Networks
320.	Paine, Tony	Kepware Technologies
321.	Pal, Partha	Raytheon BBN Technologies
322.	Palmquist, Scott	Itron
323.	Papa, Mauricio	University of Tulsa
324.	Parthasarathy, Jagan	Business Integra
325.	Patel, Chris	EMC Technology Alliances
326.	Pearce, Thomas C. II	Public Utilities Commission of Ohio
327.	Pederson, Perry	U.S. Nuclear Regulatory Commission
328.	Peters, Mike	FERC
329.	Peterson, Thomas	Boeing
330.	Phillips, Matthew	Electronic Privacy Information Center
331.	Phillips, Michael	Centerpoint Energy
332.	Phinney, Tom	
333.	Phiri, Lindani	Elster Group

	Name	Organization
334.	Pittman, James	Idaho Power
335.	Polonetsky, Jules	The Future of Privacy Forum
336.	Polulyakh, Diana	Aspect Labs
337.	Porterfield, Keith	Georgia System Operations Corporation
338.	Powell, Terry	L-3 Communications
339.	Prowell, Stacy	Oak Ridge National Laboratory
340.	Puri, Anuj	IEEE
341.	Pyles, Ward	Southern Company
342.	Qin, Andy	Cisco
343.	Qin, Jason	Skywise Systems
344.	Qiu, Bin	E:SO Global
345.	Quinn, Steve	Sophos
346.	Rader, Bodhi	FERC
347.	Radgowski, John	Dominion Resources Services, Inc
348.	Ragsdale, Gary L.	Southwest Research Institute
349.	Rakaczky, Ernest A.	Invensys Global Development
350.	Rao, Josyula R	IBM
351.	Ray, Indrakshi	Colorado State University
352.	Reddi, Ramesh	Intell Energy
353.	Revill, David	Georgia Transmission Corp.
354.	Rick Schantz	BBN
355.	Riepenkroger, Karen	Sprint
356.	Rivaldo, Alan	Public Utility Commission of Texas
357.	Rivero, Al	Telvent
358.	Roberts, Don	Southern Company Transmission
359.	Roberts, Jeremy	LonMark International
360.	Robinson, Charley	International Society of Automation
361.	Robinson, Eric	ITRON
362.	Rodriguez, Gene	IBM
363.	Rothke, Ben	National Grid
364.	Rumery, Brad	Sempra
365.	Rutfield, Craig	NTRU Cryptosystems, Inc.
366.	Rutkowska, Joanna	Invisible Things
367.	Rutkowski, Tony	Yaana Technologies
368.	Sachs, Marcus	Verizon Communications
369.	Saint, Bob	National Rural Electric Cooperative Association
370.	Sakane, Hiro	NIST
371.	Sambasivan, Sam	AT&T
372.	Sanders, William	University of Illinois
373.	Saperia, Jon	
374.	Sargent, Robert	Cisco Systems, Inc.
375.	Scace, Caroline	NIST
376.	Schantz, Rick	Raytheon BBN Technologies

	Name	Organization
377.	Scheff, Andrew	Scheff Associates
378.	Schneider, Brandon	SRA International
379.	Schulman, Ross	Center for Democracy and Technology
380.	Sconzo, Mike	Electric Reliability Council of Texas
381.	Scott, David	Accenture
382.	Scott, Tom	Progress Energy
383.	Searle, Justin	Consumers Energy / InGuardians
384.	Seo, Jeongtaek	Electronics and Telecommunications Research Institute
385.	Shastri, Viji	MCAP Systems
386.	Shaw, Vishant	Enernex
387.	Shein, Robert	EDS
388.	Sherman, Sean	Triton
389.	Shetty, Ram	General Electric
390.	Shin, Mark	Infogard
391.	Shpantzer, Gal	
392.	Silverstone, Ariel	
393.	Sinai, Nick	Federal Communications Commission
394.	Singer, Bryan	Kenexis
395.	Sisley, Elizabeth	University of Minnesota
396.	Skare, Paul	Siemens
397.	Slack, Phil	Florida Power & Light Company
398.	Smith, Brian	EnerNex
399.	Smith, Rhett	Schweitzer Engineering Laboratories, Inc.
400.	Smith, Ron	ESCO Technologies Inc.
401.	Sood, Kapil	Intel Labs
402.	Sorebo, Gilbert	SAIC
403.	Soriano, Erick	Garvey Schubert Barer
404.	Souza, Bill	
405.	Spirakis, Charles	Google
406.	Stammberger, Kurt	Mocana
407.	Starr, Christopher H.	General Dynamics Advanced Information Systems
408.	Steiner, Michael	IBM Thomas J. Watson Research Center
409.	Sterling, Joyce	NitroSecurity
410.	Stevens, James	Software Engineering Institute
411.	Stewart, Clinton	
412.	Stitzel, Jon	Burns & McDonnell Engineering Company, Inc.
413.	StJohns, Michael	Nth Permutation
414.	Stouffer, Keith	NIST
415.	Strickland, Tom	General Electric
416.	Struthers, Brent	NeuStar
417.	Stycos, Dave	Zocalo Data Systems, Ltd.
418.	Suarez, Luis Tony	Tennessee Valley Authority
419.	Suchman, Bonnie	Troutman Sanders LLP

	Name	Organization
420.	Sullivan, Kevin	Microsoft
421.	Sung, Lee	Fujitsu
422.	Sushilendra, Madhava	EPRI
423.	Swanson, Marianne	NIST
424.	Tallent, Michael	Tennessee Valley Authority
425.	Taylor, Dave	Siemens
426.	Taylor, Malcolm	Carnegie Mellon University
427.	Thanos, Daniel	General Electric
428.	Thaw, David	Hogan & Hartson
429.	Thomassen, Tom	Symantec
430.	Thompson, Daryl L.	Thompson Network Consulting
431.	Thomson, Matt	General Electric
432.	Tien, Lee	Electronic Freedom Foundation
433.	Tiffany, Eric	Liberty Alliance
434.	Toecker, Michael	Burns & McDonnell
435.	Tolway, Rich	APS
436.	Tom, Steve	Idaho National Laboratory
437.	Tran, Lan	Tangible
438.	Trayer, Mark	Samsung
439.	Truskowski, Mike	Cisco System, Inc.
440.	Turner, Steve	International Broadband Electric Communications, Inc.
441.	Uhrig, Rick	Electrosoft
442.	Urban, Jennifer	Samuelson Clinic at UC Berkeley
443.	Uzhunnan, Abdul	DTE Energy
444.	van Loon, Marcel	AuthenTec
445.	Vankayala, Vidya	BC Hydro
446.	Vayos, Daphne	Northeast Utilities
447.	Veillette, Michel	Trilliant Inc.
448.	Veltsos, Christophe	Minnesota State University
449.	Venkatachalam, R. S.	Mansai Corporation
450.	Vettoretti, Paul	SBC Global
451.	Wacks, Kenneth P.	Massachusetts Institute of Technology
452.	Waheed, Aamir	Cisco Systems, Inc.
453.	Walia, Harpreet	Wave Strong Inc.
454.	Wallace, Donald	Itron
455.	Walters, Keith	Edison Electric Institute
456.	Walters, Ryan	COO TerraWi Communications
457.	Wang, Alex	Cisco Systems, Inc.
458.	Wang, Longhao	Samuelson Clinic at UC Berkeley
459.	Wang, Yongge	University of North Carolina-Charlotte
460.	Watson, Brett	NeuStar
461.	Wei, Dong	SIEMENS Corporation
462.	Wepman, Joshua	SAIC Commercial Business Services

	Name	Organization
463.	West, Andrew C	Invensys Process Systems
464.	Weyer, John A.	John A. Weyer and Associates
465.	Whitaker, Kari	LockDown, Inc.
466.	White, Jim	Uniloc USA, Inc.
467.	Whitney, Tobias	The Structure Group
468.	Whyte, William	Ntru Cryptosystems, Inc.
469.	Williams, Terron	Elster Electricity
470.	Wingo, Harry	Google
471.	Witnov, Shane	University of California, Berkeley
472.	Wohnig, Ernest	Booz-Allen Hamilton
473.	Wolf, Dana	RSA
474.	Worden, Michael	New York State Public Service Commission
475.	Worthington, Charles	Federal Communications Commission
476.	Wright, Andrew	N-Dimension Solutions
477.	Wright, Josh	Inguardians
478.	Wu, Lei	
479.	Wyatt, Michael	ITT Advanced Technologies
480.	Yan, Victoria	Booz Allen Hamilton
481.	Yao, Taketsugu	Oki Electric Industry, Co., Ltd
482.	Yardley, Tim	University of Illinois
483.	Yoo, Kevin	Wurldtech
484.	Zurcher, John	SRA