This publication is available free of charge from http://dx.doi.org/10.6028/NIST.IR.7628r1

NISTIR 7628 Revision 1

Guidelines for Smart Grid Cybersecurity

Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements

The Smart Grid Interoperability Panel –
Smart Grid Cybersecurity Committee

http://dx.doi.org/10.6028/NIST.IR.7628r1

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

NISTIR 7628 Revision 1

Guidelines for Smart Grid Cybersecurity

Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements

The Smart Grid Interoperability Panel–
Smart Grid Cybersecurity Committee

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.7628r1

September 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology Interagency Report 7628 Rev. 1, Vol. 1
290 pages (September 2014)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: NISTIR.7628.Rev1@nist.gov

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 analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This three-volume report, *Guidelines for Smart Grid Cybersecurity*, presents an analytical framework that organizations can use to develop effective cybersecurity 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 cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

Keywords

advanced metering infrastructure; architecture; cryptography; cybersecurity; electric grid; privacy; security requirements; smart grid

ACKNOWLEDGMENTS

This revision to the NISTIR was developed by members of the Smart Grid Interoperability Panel (SGIP) Smart Grid Cybersecurity Committee (SGCC) (formerly the Cyber Security Working Group (CSWG)), which is chaired by Victoria Yan Pillitteri (NIST). Dave Dalva (Stroz Friedberg), Akhlesh Kaushiva (Department of Energy), and Scott Saunders (Sacramento Municipal Utility District) are the vice chairs and Mark Enstrom (Neustar) and Amanda Stallings (Ohio PUC) have served as the secretary. Tanya Brewer of NIST is the lead editor of this report. A special note of thanks goes to the subgroup leads, Frances Cleveland (Xanthus Consulting International), Nelson Hastings (NIST), Rebecca Herold (Rebecca Herold & Associates, LLC), Elizabeth Sisley (Calm Sunrise Consulting, LLC), and Doug McGinnis (Exelon) who along with their subgroup team members contributed significantly to this revision. The dedication and commitment of all the individuals in developing the original document and now this revision is significant, especially the leadership of Marianne Swanson (NIST), who previously chaired the group. In addition, appreciation is extended to the various organizations that have committed these resources to supporting this endeavor. Past and current members of the SGCC/CSWG are listed in Appendix K of this report.

Acknowledgement is also extended to the NIST Smart Grid Team and to Liz Lennon (NIST) for her superb technical editing of this report. Thanks is also extended to Bruce McMillin (Missouri University of Science and Technology), and to Harold Booth and Quynh Dang (NIST) for assistance in updating specific sections in the document. 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 Cybersecurity*, presents an analytical framework that organizations can use to develop effective cybersecurity 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 cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

The initial version and this revision of the *Guidelines for Smart Grid Cybersecurity* were 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 new SGIP, which has transitioned to a member-funded non-profit organization, has renamed the CSWG to the Smart Grid Cybersecurity Committee (SGCC). The SGCC has 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 the SGIP 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. The SGIP transitioned to a member-funded non-profit organization in January 2013. For information on the new SGIP organization, see: http://www.sgip.org.

This document is a companion document to the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0* (NIST Special Publication 1108),[2] which NIST issued in February 2012. The Framework 2.0 document lays out a plan for transforming the nation's aging electric power system into an interoperable smart grid—a network that will integrate information and communication technologies with the power-delivery infrastructure, enabling two-way energy and communications flow. This document reflects input from a wide range of stakeholder groups, including representatives from trade associations, standards organizations, utilities, and industries associated with the power grid. The document reflects the consensus-based process the SGIP uses to coordinate and accelerate the development of smart grid standards. The Framework 2.0 version adds 22 standards, specifications, and guidelines to the 75 standards NIST recommended as being applicable to the smart grid in the 1.0 version of January 2010. The improvements and additions to the 1.0 version include:

- a new chapter on the roles of the SGIP;
- an expanded view of the architecture of the smart grid;
- a number of developments related to ensuring cybersecurity for the smart grid, including a Risk Management Framework for the electricity subsector to provide guidance on security practices;
- a new framework for testing the conformity of devices and systems to be connected to the smart grid—the Interoperability Process Reference Manual;
- information on efforts to coordinate the smart grid standards effort for the United States with similar international efforts; and
- an overview of future areas of work, including electromagnetic disturbance and interference, and improvements to SGIP processes.

The SGCC will continue to provide additional guidance as the Framework document is updated and expanded, and as additional standards are identified by NIST.

This document (the original NIST Interagency Report and Revision 1) is the product of a participatory public process that, starting in March 2009, included workshops as well as weekly and bi-weekly teleconferences, all of which were open to all interested parties. Drafts of the three volumes will have undergone at least one round of formal public review before final publication. The public review cycle will be announced in The Federal Register in advance.

The three volumes that make up this initial set of guidelines are intended primarily for individuals and organizations responsible for addressing cybersecurity 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.

[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 2.0 (NIST SP 1108R2)*, Feb. 2012, available: http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf [accessed 8/11/2014].

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 cybersecurity.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements
  - Chapter 1
    Document *Development Strategy* includes background information on the smart grid and the importance of cybersecurity in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the cybersecurity strategy for the smart grid and the specific tasks within this strategy.
  - Chapter 2
    Logical *Architecture and Interfaces of the Smart Grid*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 Cybersecurity Documents*
  - Appendix B – *Example Security Technologies and Services 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 provides an overview of some existing privacy risk mitigation standards and frameworks. Also includes a description of some methods that can be used to mitigate privacy risks, and points to privacy use cases.
  - Appendix C – *Changing Regulatory Frameworks*
  - Appendix D – *Recommended Privacy Practices for Customer/Consumer Smart Grid Energy usage Data Obtained Directly by Third Parties*
  - Appendix E – *Privacy Use Cases*
  - Appendix F - *Summary of the Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment*

  - Appendix G – *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.
  - Chapter 8 – *Research and Development Themes for Cybersecurity 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 H – *Analysis Matrix of Logical Interface Categories*
  - Appendix I – *Mappings to the High-Level Security Requirements*
  - Appendix J – *Glossary and Acronyms*
  - Appendix K – *SGIP-CSWG and SGIP 2.0 SGCC Membership*

CHAPTER 1
DOCUMENT DEVELOPMENT 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 cybersecurity of systems and information in the IT and telecommunications infrastructures must be addressed by an evolving electric sector. Cybersecurity must be included in all phases of the system development life cycle, from design phase through implementation, maintenance, and disposition/sunset.

Cybersecurity 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. In Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, issued in February 2013, it was recognized that the

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.[3]

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

[3] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf [accessed 8/11/2014].

- 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 cybersecurity 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, cybersecurity for the power industry covers all issues involving automation and communications that affect the operation of electric power systems, 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 should also be addressed, and the focus should be an all-hazards approach.

Development of the *Guidelines for Smart Grid Cybersecurity* 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). This group was renamed under the Smart Grid Interoperability Panel (SGIP) as the Cyber Security Working Group (SGIP-CSWG) in January 2010. In January 2013, the SGIP became a privately funded organization, and the CSWG was renamed the Smart Grid Cybersecurity Committee (SGCC). The SGCC has participants from the private sector (including vendors and service providers), manufacturers, various standards organizations, academia, regulatory organizations, and federal agencies.

This document addresses cybersecurity using a thorough process that results in a high-level set of cybersecurity requirements. These requirements were developed (or augmented, where standards/guidelines already exist) using a high-level risk assessment process that is defined in the cybersecurity strategy section of this report. Cybersecurity requirements are implicitly recognized as critical in all of the priority action plans discussed in the updated Special Publication (SP), *NIST Framework and Roadmap for Smart Grid Interoperability Standards,* Release 2.0 (NIST SP 1108R2), which was published in February 2012.

Just like in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* Release 2.0 lays out a plan for transforming the nation's aging electric power system into an interoperable smart grid—a network that will integrate information and communication technologies with the power-delivery infrastructure, enabling two-way flows of energy and communications. This document reflects input from a wide range of stakeholder groups, including representatives from trade associations, standards organizations, utilities, and

industries associated with the power grid. The document reflects the consensus-based process the SGIP uses to coordinate development of smart grid standards. Just as its earlier version did, the Framework 2.0 adds 22 standards, specifications, and guidelines to the 75 standards NIST recommended as being applicable to the smart grid in the 1.0 version of January 2010. The improvements and additions to the 1.0 version include:

- a new chapter on the roles of the SGIP;
- an expanded view of the architecture of the smart grid;
- a number of developments related to ensuring cybersecurity for the smart grid, including a Risk Management Framework to provide guidance on security practices;
- a new framework for testing the conformity of devices and systems to be connected to the smart grid—the Interoperability Process Reference Manual;
- information on efforts to coordinate the smart grid standards effort for the United States with similar efforts in other parts of the world; and
- an overview of future areas of work, including electromagnetic disturbance and interference, and improvements to SGIP processes.

This document expands upon the discussion of cybersecurity included in the Framework document. NIST Interagency Report (NISTIR) 7628 is a starting point and a foundation for smart grid cybersecurity. The SGCC will continue to provide additional guidance as the Framework document is updated and expanded, and as additional standards are identified by NIST.

This document is a tool for organizations that are researching, designing, developing, and implementing smart grid technologies. The cybersecurity strategy, risk assessment process, and security requirements included in this document should be applied to the entire smart grid system.[4]

Cybersecurity risks should be addressed as organizations implement and maintain their smart grid systems.[5] Therefore, this document may be used as a guideline to evaluate the overall cyber risks to a smart grid system during the design, system implementation and maintenance phases. 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 helps secure and meet the reliability requirements of the electric grid. In May 2012

[4] NISTIR 7628 does not impose any actual requirements on any person or entity. Any application or implementation of any "requirements" referenced in NISTIR 7628 or any assessment thereof will be self-imposed, imposed by contract between the relevant parties, or imposed by the applicable regulatory authority if, and to the extent, separately determined to be so imposed.

[5] A smart grid system may consist of IT which is a discrete system of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A smart grid system may also consist of operational technologies (OT) or industrial control systems (ICS), which is a general term that encompasses several types of operational and control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures.

the *Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*[6] was developed by the Department of Energy (DOE), in collaboration with NIST and the North American Electric Reliability Corporation (NERC). The RMP was written with the goal of enabling electricity subsector organizations— regardless of size or organizational or governance structure—to apply effective and efficient risk management processes and tailor them to meet their organizational requirements. This guideline may be used to implement a new cybersecurity program within an organization or to build upon an organization's existing internal cybersecurity policies, standard guidelines, and procedures.

1.1 CYBERSECURITY AND THE ELECTRIC SECTOR

The critical role of cybersecurity in ensuring the effective operation of the smart grid is documented in legislation and in the DOE 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity.* 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.
>
> * * * * * * * *

Cybersecurity for the smart grid supports both the reliability of the grid and the confidentiality (and privacy) of the information that is transmitted.

Recognizing that the national and economic security of the United States depends on the reliable functionality of critical infrastructure, the President under Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[7] has directed NIST to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. The resulting Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)[8] consists of standards, guidelines, and best practices to promote the protection of critical infrastructure, including the electricity subsector and the smart grid. The prioritized, flexible, repeatable, and cost-effective approach of the Cybersecurity Framework will help owners and operators of critical infrastructure to manage cybersecurity-related risk while protecting business confidentiality, individual privacy, and civil liberties. The Cybersecurity Framework, published in February 2014, serves as a national-level framework that is flexible enough to apply across multiple sectors. The Cybersecurity Framework has been developed based on stakeholder input to help ensure that existing work within the sectors, including the electricity subsector, can be

---

[6] U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process,* DOE/OE-0003, May 2013, 96 pp. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf [accessed 8/11/2014].

[7] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf [accessed 8/11/2014].

[8] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0, February 12, 2014, 41 pp.http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 8/11/2014].

utilized within the Framework. Existing smart grid cybersecurity standards, guidelines, and practices can be leveraged to address the Cybersecurity Framework in the context of an organization's risk management program.

1.2 SCOPE AND DEFINITIONS

Developed as an update to the 2006 *Roadmap to Secure Control Systems in the Energy Sector*, the 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity*[9] outlines a strategic framework over the next decade among industry, vendors, academia and government stakeholders to design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber incident while sustaining critical functions.

Traditionally, cybersecurity for IT focuses on the protection required to ensure the confidentiality, integrity, and availability of the electronic information communication systems. Cybersecurity 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. Cybersecurity in the smart grid should 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 addition, safety and reliability are of paramount importance in electric power systems. Any cybersecurity measures in these systems must not impede safe, reliable power system operations.

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

- The smart grid and cybersecurity;
- Technologies and their use in power systems; and
- Our understanding of the risk environment in which those technologies operate.

This document 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.

[9] U.S. Department of Energy, Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011, 80 pp. http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf [accessed 8/11/2014].

Finally, this document 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 CYBERSECURITY DOCUMENT DEVELOPMENT STRATEGY

The overall strategy used 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 strategy addressed prevention, detection, response, and recovery. This overall strategy is potentially applicable to other complex infrastructures.

The document development strategy required the definition and implementation of an overall cybersecurity 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 document is guidance for organizations. NIST does not prescribe particular solutions through the guidance contained in this document. Each organization must develop its own detailed cybersecurity approach (including a risk assessment methodology) for the smart grid.

Parts of the following documents were used in developing the risk assessment process for the smart grid:[10]

- NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST, March 2011;
- 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*, version 1.0, NERC, June 14, 2002;

[10] Note that many of the documents listed have been updated since the initial development of the smart grid cybersecurity risk assessment process.

- *The National Infrastructure Protection Plan, Partnering to enhance protection and resiliency***,** Department of Homeland Security (DHS), 2009;
- The IT, telecommunications, and energy sector-specific plans (SSPs), initially published in 2007 and updated annually;
- ANSI/ISA-62443-1-1 (99.01.01)-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, International Society of Automation (ISA), 2007[11]; and
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, ISA, January 2009[12].

The next step in the document development strategy was to select and modify (as necessary) the cybersecurity requirements. The cybersecurity 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 does not prescribe particular solutions to cybersecurity issues through the guidance contained in this document.

The cybersecurity issues that an organization implementing smart grid functionality should address are diverse, complex, and will vary across organizations. This document includes an approach for assessing cybersecurity issues and selecting and modifying cybersecurity 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 cybersecurity 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 document development strategy for the smart grid were undertaken by participants in the CSWG/SGCC. The remainder of this subsection describes the tasks that have been performed in the implementation of the document development 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 used to develop this smart grid cybersecurity document. The tasks are defined following the figure.

[11] https://www.isa.org/store/products/product-detail/?productId=116720.
[12] https://www.isa.org/store/products/product-detail/?productId=116731.

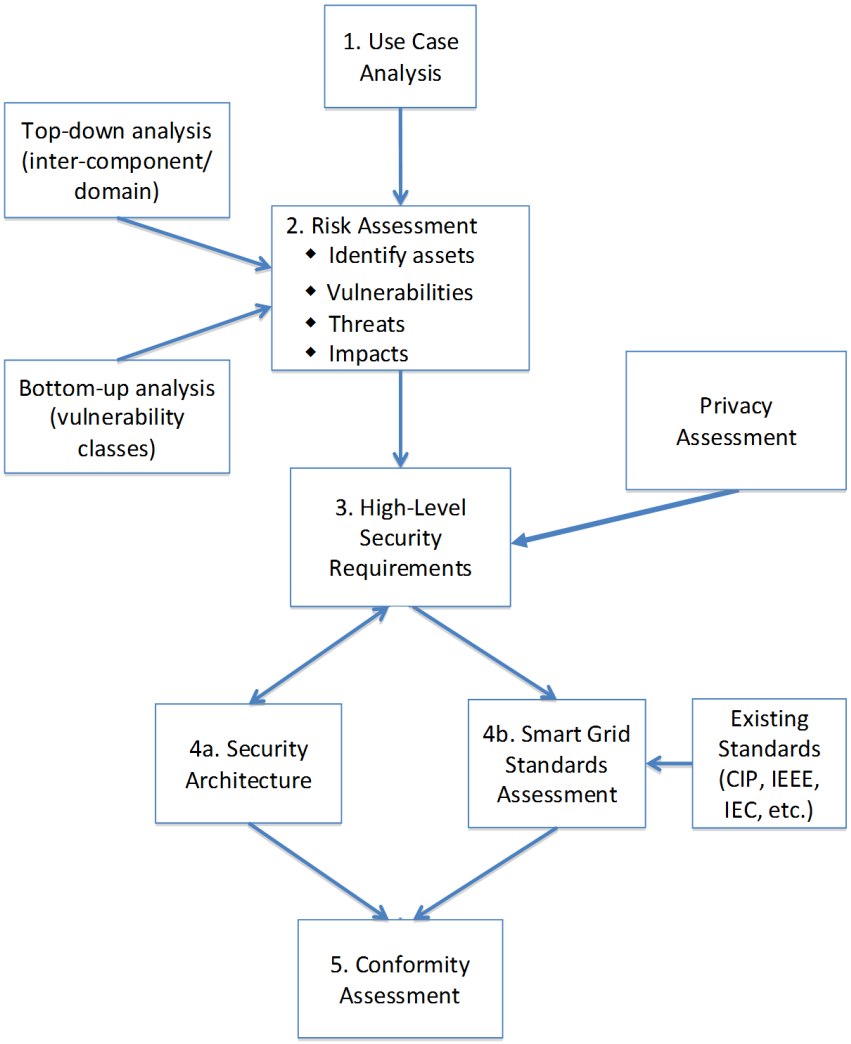


Figure 1-1 Tasks in the Smart Grid Cybersecurity Document Development Strategy

Task 1. Selection of use cases with cybersecurity considerations.[13]

The use cases included in Chapter 10 of this document 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.

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.

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

Vulnerability classes: The initial list of vulnerability classes[14] was developed using information from several existing documents and web sites, e.g., NIST SP 800-82, *Guide to Industrial Control Systems Security*, 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 cybersecurity 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.[15] 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 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.

[14] 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.

[15] The definitions of low, moderate, and high impact are found in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

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 cybersecurity experts and power system experts were needed. The cybersecurity 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 cybersecurity requirements in this report[16]—

- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009;[17]

[16] NIST SP 800-53 is mandatory for federal agencies, and the NERC CIPs are mandatory for the Bulk Power System. This report, NISTIR 7628 Rev. 1, is a guidance document and is not a mandatory standard.

[17] At the time the high-level security requirements were specified, NIST SP 800-53 Rev. 3 was required for federal agencies. At the date of publication of this revision, NIST SP 800-53 Rev. 4 has superseded Rev. 3 and is available at: http://dx.doi.org/10.6028/NIST.SP.800-53r4

- NERC CIP-002 through -009, version 2;[18]
- *Catalog of Control Systems Security: Recommendations for Standards Developers*, DHS, April 2011; and
- Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) security profiles.[19]

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 A of this report, 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 into one of three categories that were developed for this document: 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 should determine the logical interface categories[20] 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, such as safety measures, may be used to meet specific security requirements.

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 high-level security requirements specified in Chapter 3.

[18] At the time the high-level security requirements were specified, NERC CIP v2 was mandatory and enforceable. At the date of publication of this revision, NERC CIP v3 is now mandatory and enforceable and can be obtained from the following URL: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[19] Publicly available versions of ASAP-SG documentation may be found athttp://www.utilisec.com/resources/.

[20] For more on the logical interface categories (LICs) see §2.3 Logical Interface Categories.

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.

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 are assessed to determine relevancy to smart grid security. In this process, gaps in security requirements are identified and recommendations are made for addressing these gaps. Also, conflicting standards and standards with security requirements not consistent with the security requirements included in this report are identified with recommendations.

Task 5. Conformity Assessment.

The final task is to develop a conformity assessment program for security. The SGIP Smart Grid Testing and Certification Committee (SGTCC) developed and issued an *Interoperability Process Reference Manual* (IPRM) Version 2.0[21] in January 2012 that details its recommendations on processes and best practices that enhance the introduction of interoperable and secure products in the marketplace. These recommendations build upon international standards-based processes (ISO/IEC[22] 17025 and ISO/IEC Guide 65) for interoperability testing and certification for testing laboratories and certification body management systems.

1.4 COMBINED CYBER-PHYSICAL ATTACKS

As described in the original version of this document, addressing combined cyber-physical attacks is an ongoing effort by the SGCC in coordination with the public and private sectors. Cyber-physical attacks, also called blended attacks, are executed by an adversary or result from inadvertent action that cause a greater impact and/or different consequences than a cyber or physical attack could cause individually. In order to address the enhanced impacts generated by these blended attacks, the risks and vulnerabilities for both cyber and physical attacks must be considered. The high-level security requirements presented in this chapter address the impact of cyber vulnerabilities; however, by selecting and tailoring an appropriate subset of requirements, it is possible to also address some physical vulnerabilities of the power grid. NIST SP 800-82 Rev. 1, *Guide to Industrial Control Systems Security*, and ISA 99, *Industrial Automation and Control Systems Security*, are additional resources that may be leveraged to help address cyber-physical attack.

[21] *IPRM Version 2.0*, January 2012. https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SmartGridTestingAndCertificationCommittee/IPRM_final_-_011612.pdf

[22] International Organization for Standardization / International Electrotechnical Commission

Cyber-physical attacks can be classified into three broad subsets:

1. **Physical attacks informed by cyber** – The use of information gathered by cyber means that allows an adversary to plan and execute an improved or enhanced physical attack. For instance, an adversary has decided to destroy components within a substation though they are not sure which substation or components would have the greatest impact. If they could access confidential information or aggregate unprotected information by cyber means that tells them that a particular substation is on a very congested path and which lines were at their maximum ratings, they could then physically attack that specific substation and lines. This could cause a much greater impact than the attack of a random substation.
2. **Cyber attacks enhancing physical attacks** – An adversary uses cyber means to improve or enhance the impacts of a physical attack by either making the attack more successful (e.g., greater consequences) or interfering with restoration efforts (thereby increasing the duration of the attack). Although the term "adversary" is used, inadvertent actions could also cause such an attack.
   One example is an adversary tampering with the integrity of protective relay settings prior to a physical attack on power lines. Although the original settings were designed to contain the effects of a failure, the tampered settings allow the failure to cascade into impacts on a wider segment of the grid.

   Another example is after a physical attack, an adversary performing DoS attacks on the availability of systems and facilities that support restoration activities. These attacks disrupt the restoration, prolonging the resulting outages.
3. **Use of a cyber system to cause physical harm** – An adversary uses a cyber system that controls physical equipment in such a manner to cause physical harm/damage. An example of this is the burner management system for a natural gas generator. In this case, an adversary or a careless operator could attempt to turn on the natural gas inflow without an ignition source present. As the burner unit fills with natural gas, the adversary could turn on the ignition source, potentially causing an explosion.

Cyber-physical attacks can greatly enhance the overall impact and/or consequences of an attack or increase the duration of those consequences by delaying or interfering with responses. However, good cyber, physical, and operational security planning and implementations can minimize these impacts. Defensive measures that can be used to minimize the likelihood of successful cyber attacks and physical attacks will also work to minimize the impacts of a cyber-physical attack. Security operators need to consider both types of attacks and how they may be used together in order to better develop systems that are resilient to cyber-physical attacks. The application of NISTIR 7628 and other security standards and guidelines as part of an organization-wide risk management process can help reduce the cyber vulnerabilities and limit the impacts of cyber-physical attacks.

CHAPTER 2
LOGICAL ARCHITECTURE AND INTERFACES OF THE SMART GRID

This chapter includes a logical reference model of the smart grid[23], including all the major domains—service providers, customer, transmission, distribution, bulk generation, markets, and operations—that are part of the NIST conceptual model.

Figure 2-3 presents the logical reference model and represents a composite high-level view of smart grid domains and actors, initially created prior to the formation of the SGAC. The information in this report is presented as guidance on cybersecurity, but is neither prescriptive nor does it restrict innovation. 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.[24] 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. 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 systems and components of the smart grid. The list of actors is a subset of the full list of actors

[23] The SGCC Architecture Subgroup began coordination and harmonization efforts with the SGIP Architecture Committee (SGAC) and the European Union's Smart Grid Coordination Group Reference Architecture Working Group

[24] This was previously named Demand Response.

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, 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.

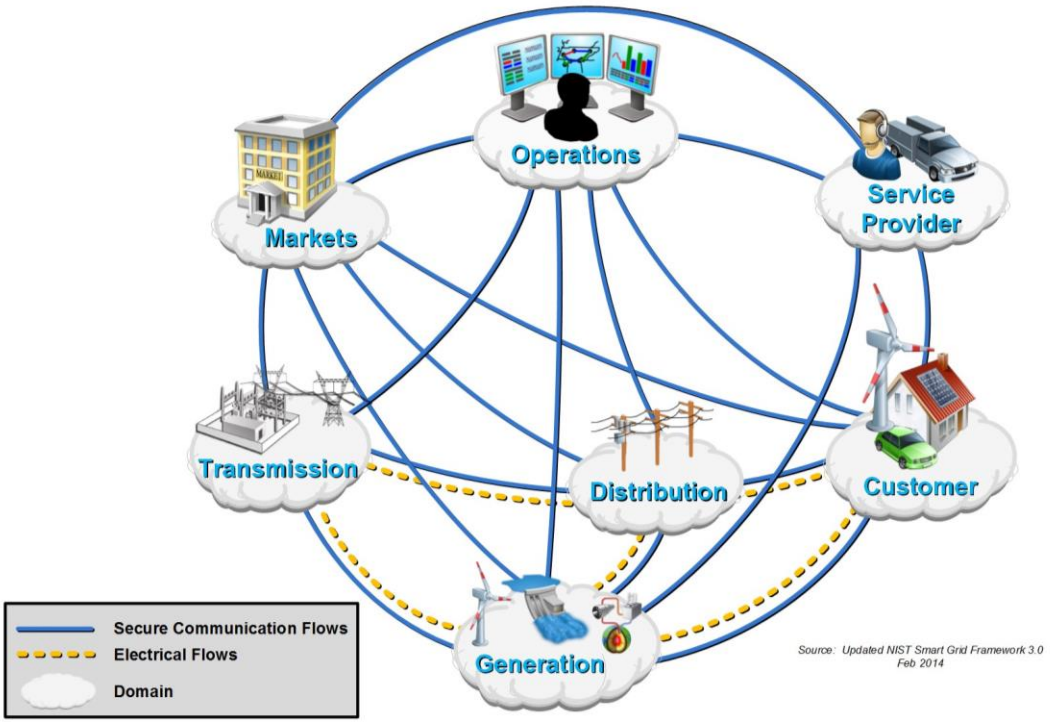


Figure 2-1 Interaction of Actors in Different Smart Grid Domains through Secure Communication Flows

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.

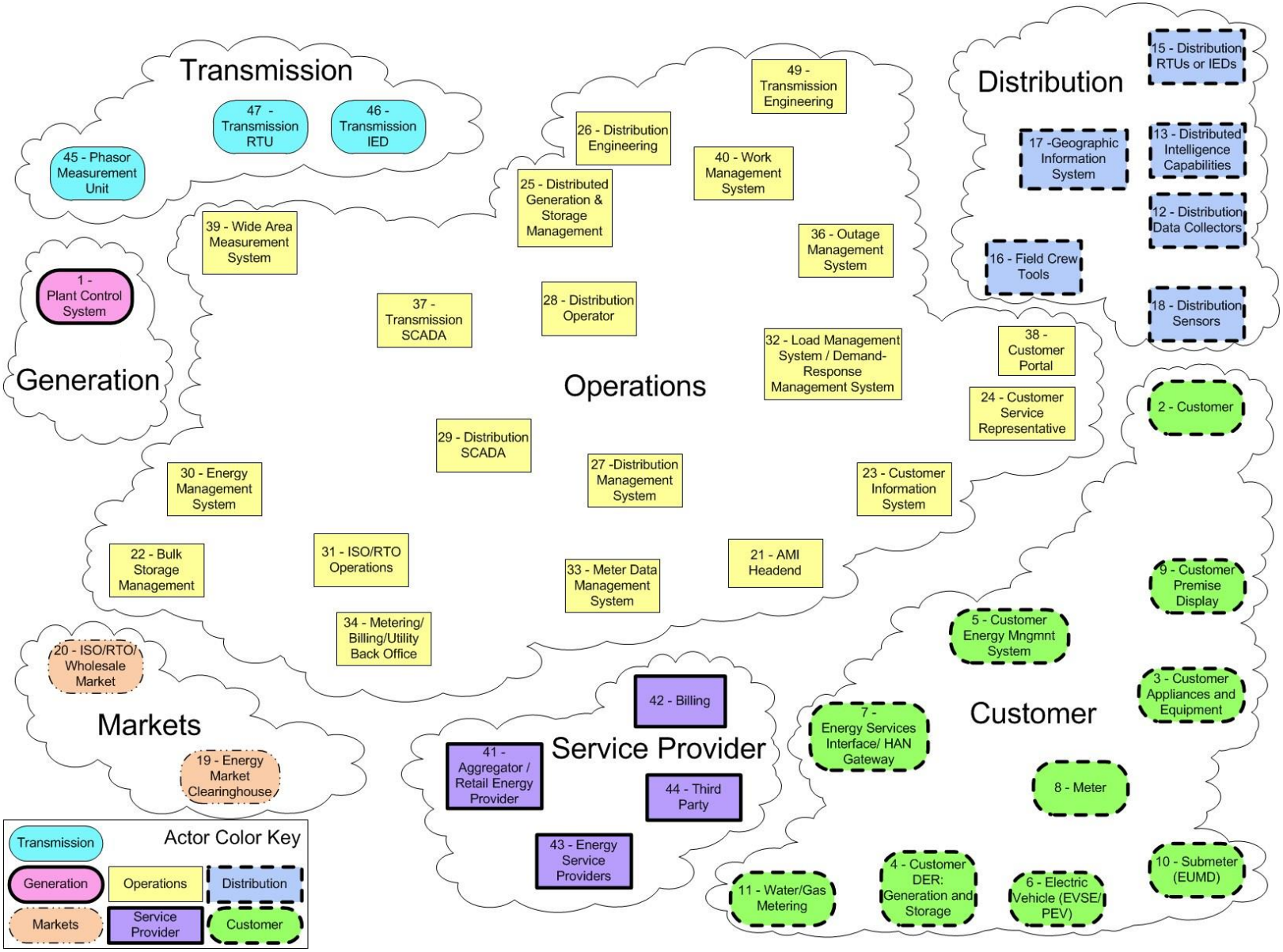


Figure 2-2 Composite High-level View of the Actors within Each of the Smart Grid Domains

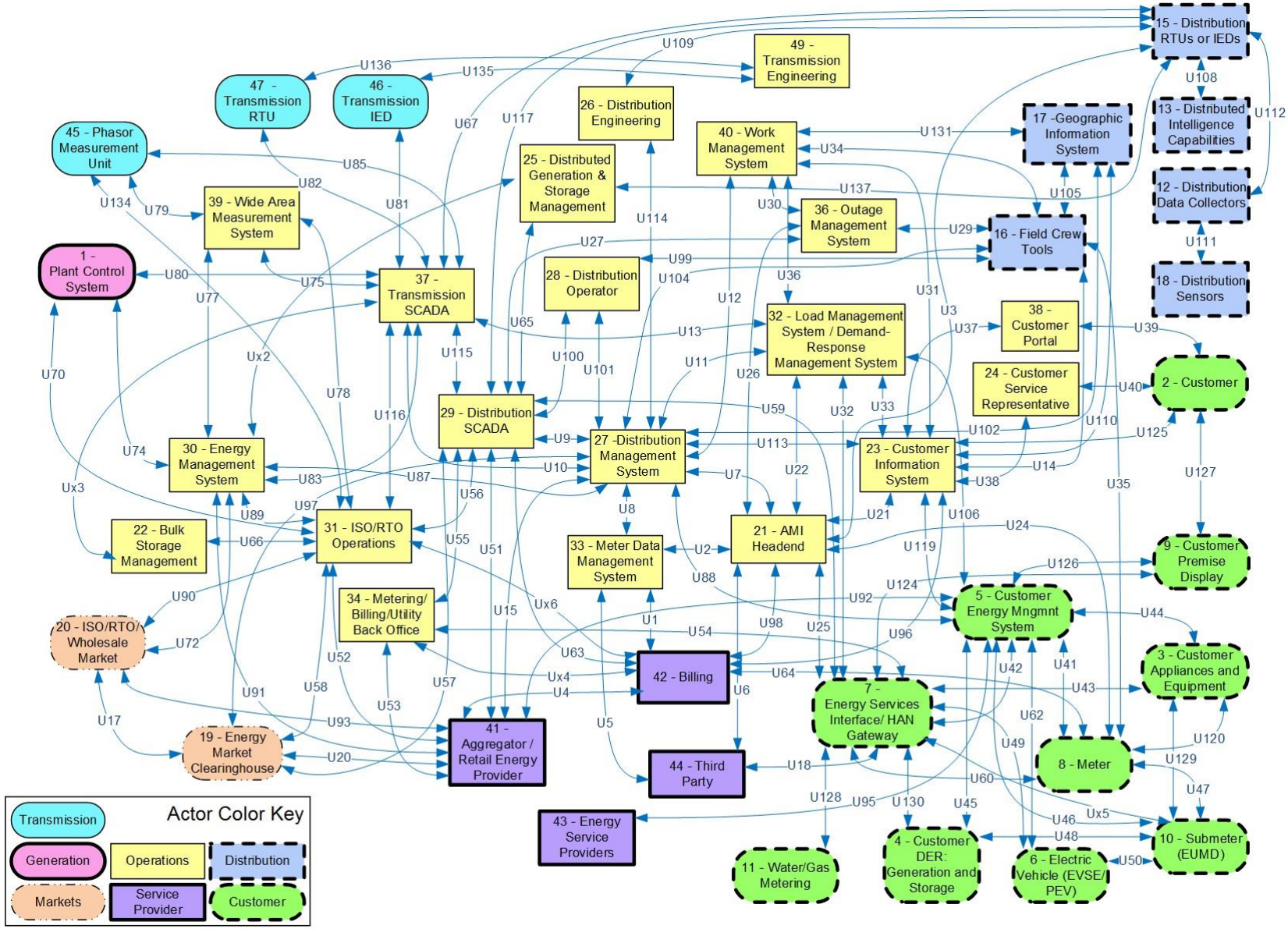


Figure 2-3 Logical Reference Model

Table 2-1 Actor Descriptions for the Logical Reference Model

Actor Number	Domain	Actor	Acronym	Description
1	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 (home area network/business area network (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	Plug-in Electric Vehicle/ Electric Vehicle Service Element	PEV/ EVSE	A PEV is a vehicle propelled by an electric motor and powered by a rechargeable battery. It can be recharged using an external power source. When the external power source is the power grid, the EV is connected through the EVSE that provides power and communication.
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.

Actor Number	Domain	Actor	Acronym	Description
8	Customer	Meter		Point of sale device used for the transfer of product and measuring usage from one domain/system to another.
9	Customer	Customer Premise Display		A device that displays usage and cost data to the customer on location.
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		A 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. .
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.
15[25]	Distribution	Distribution Remote Terminal Unit/Intelligent Electronic Device	RTUs or IEDs	Receives data from sensors and power equipment, and can issue control commands, such as tripping circuit breakers, if voltage, current, or frequency anomalies are identified, RTUs and/or IEDs can raise/lower voltage levels to maintain the desired voltage range.
16	Distribution	Field Crew Tools		A field engineering and maintenance tool set that includes 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 that can be read by an observer or by an instrument.

[25] Actor 14 was removed during further development of the reference model.

Actor Number	Domain	Actor	Acronym	Description
19	Markets	Energy Market Clearinghouse		Wide area energy market operation system providing high-level market signals for distribution companies (ISO/RTO and Utility Operations).
20	Markets	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.
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.
22	Operations	Bulk Storage Management		Provides management for 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]).
25	Operations	Distributed Generation and Storage Management		Distributed generation is the process of generating electricity from many small, local energy sources. Storage management enables the efficient integration of distributed generation sources into the grid.
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.

Actor Number	Domain	Actor	Acronym	Description
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 supervisory computerized system that that gathers and processes data and applies operational controls for distribution-side systems used to control dispersed assets.
30	Operations	Energy Management System	EMS	A system used by electric grid operators to monitor, control, and optimize the performance of the generation and/or transmission system.
31	Operations	ISO/RTO Operations		Wide area power system control center providing high-level load management and security analysis for the transmission grid, typically using an 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.'
34	Operations	Metering/Billing/Utility Back Office		Back office utility systems for metering and billing.

Actor Number	Domain	Actor	Acronym	Description
36[26]	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		A supervisory computerized system that gathers and processes data (e.g., transmitting device status) and applies operational controls (e.g., manages energy consumption by controlling compliant devices) for transmission-side systems used to control dispersed assets.
38	Operations	Customer Portal		The online interface through which a customer can interact with the energy service provider. 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.
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.

[26] Actor 35 was deleted during development

Actor Number	Domain	Actor	Acronym	Description
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		An entity that performs the function of generating an invoice to obtain payment 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	A device that 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 Intelligent Electronic Device (IED)		A device that receives data from sensors on the power network 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 Remote Terminal Unit (RTU)		A remote terminal unit passes status and measurement information from a transmission substation or feeder equipment to a SCADA system and transmit control commands sent from the SCADA system to the field equipment.
48[27]	Operations	Security/Network/System Management		An entity that monitors and configure the security, network, and system devices.
49	Operations	Transmission Engineering		A technical function of planning or managing the design or upgrade of the transmission system (e.g., equipment designed for more than 345,000 volts between conductors).

[27] Actor 48 is included in logical interface category 22 for security. It is not included in the rest of 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 will be critical to interoperability and reliability, will communicate bi-directionally, and will be tasked with maintaining confidentiality, integrity, and availability (CIA) vital to power systems operation.

The definitions of CIA are defined in federal statutes 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 needs to provide security.

This report has identified cybersecurity requirements for the different logical interface categories. Included in Appendix B are categories of cybersecurity 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 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. Fundamental concepts are that people, process, and technology are all necessary; any element alone can be circumvented. This is often referred to as "defense-in-depth." For the electric sector, geographic distances (i.e., outside of the data center) and substations are additional challenges. Section 2.2.2 contains additional detail.
- **Defense-in-breath strategy:** Security activities that are planned across the system, network, or subcomponent life cycle: product design and development, manufacturing, packaging, assembly, system integration, distribution, operations, maintenance, and

retirement. The goal is to identify, manage, and reduce the risk of exploitable vulnerabilities across the life cycles.[28]

- **Power system availability:** The primary focus of power systems engineering and operations is supporting the safe and reliable delivery of electricity. 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 cybersecurity requirements.
- **Microgrids:** Implied hierarchy in availability and resilience eliminates potential peer-to-peer negotiations between microgrids. Microgrid models suggest that availability starts in a local microgrid and that resilience is gained by aggregating and interconnecting those microgrids. These interactions are not just theoretical. Microgrids are intended to operate either as islands or interconnected; islands are key where critical operations need to be maintained.
- **Wide Area Situation Awareness (WASA)**: WASA is often shared between business entities; such information should be specified and secured in accord with principles of Service-oriented Architecture (SOA) security. Examples of such interactions might include exchange of WASA between provider and aftermarket consumer (Co-op or Aggregator), between utility and emergency management, or between adjacent bulk providers.

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 cybersecurity 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.
6. As is common practice, the existing legacy systems will need to be considered as the new architecture is designed. Security implications will need to be reviewed and updated, both to consider the legacy security mechanisms and the current state of security practice.

[28] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011.

2.2.2 Defense-in-Depth Overview

A defense-in-depth approach focuses on defending the information (including customer information), assets, power systems, and communications and IT infrastructures through layered defenses (e.g., firewalls, intrusion detection systems, antivirus software, and cryptography). It is expected that multiple levels of security measures will be implemented, both 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.

A defense-in-depth strategy requires a balanced approach with a focus on three critical elements: 1) people, 2) process, and 3) technology (See Figure 2-4) because each element alone can be circumvented. Training is critical, and protection points are shown in the following diagram. The goal of a proper defense-in-depth strategy is to make the attackers' job much more difficult, to slow the attacker down, and allow the victim to be alerted to unauthorized activity in time to prevent harm to the organization.

Figure 2-4 An Example of Defense-In-Depth

Due to the interconnected nature of the smart grid systems, it is essential that the appropriate cybersecurity controls get implemented to protect against less-critical systems infecting more-critical systems. Physical security controls such as locked doors, locked cabinets, and or restricted areas are used to mitigate risk. Other physical security controls, such as closed circuit TV, card readers, etc., are used to monitor and log entry into restricted areas.

Cybersecurity services (i.e., safeguards or countermeasures), mechanisms, and objects should be applied in layers, with one or more security methods implemented at each layer. The primary objective of these methods is to mitigate the risk of one component of the defensive strategy being compromised or circumvented. This is often referred to as "defense-in-depth." A defense-in-depth approach focuses on the following areas:

1. **Defense in multiple places** – An organization should deploy cybersecurity services, mechanisms and objects at multiple locations to resist all attack approaches.
   - **Security Services** - Functions that, when provided in a systems environment, serve to ensure the protection of resources by enforcing the defined security policies of the organization. Security services are also known as security controls, requirements, safeguards, countermeasures, and dimensions.
   - **Security Mechanisms** - The technical tools used to implement the security services listed above. Each of the security mechanisms may operate individually, or in concert with others.
   - **Security Objects** – These are items that contain security relevant information about users, groups, privileges, policies, programs, passwords, encryption keys, audit logs, etc. Managed security objects describe what is managed and how it behaves. The definition of managed security objects includes specification of their attributes and their behavior, which provides a concrete description of what is manageable.

   The "how" of management is defined by managing objects consisting of applications and data, which support the management and use of the rest of the system. This grouping, or security domain, refers to the set of entities (security objects) that are under the scope of a single organization's set of security policies.
2. **Layered defenses** – There is no such thing as 100% security. All cybersecurity approaches have inherent vulnerabilities. Creating layered defenses (firewalls, data diodes, etc.) are ways to protect against these vulnerabilities.
3. **Security robustness** – Cybersecurity components should have specified robustness (strength and assurance) as a function of the criticality and risk of what is being protected (i.e., the SCADA system, AMI meters, etc.). Examples that increase security robustness include system hardening, antivirus software, patching, etc.
4. **Trust relationships -** Trust relationships between systems and organizations need to be evaluated, established, and maintained based on the risk presented to the interfacing systems, the functions they support, and the grid as a whole; accounting for potential impact as the data may subsequently be directly or indirectly passed "deeper" into more protected levels. The potential impact is the basis for deciding on the wisdom of the connection, the security services selected, and the audit of attached system security services and related management processes. Roles and responsibilities need to be defined for the trusted partners, for example who will patch updates and on what schedule, who has system privileges, or who will purchase components from which suppliers.
5. **Deployment of cryptographic infrastructure** – Supporting key, privilege, and certificate management that enables positive identification of entities using information and communication technologies.
6. **Deployment of intrusion detection/prevention systems** – Provision of detection, reporting, analysis, assessment and response infrastructure enabling rapid detection and response to intrusions and other anomalous events, and providing situational awareness of the electric grid.

7. **Skilled staff** - A comprehensive program of education, training, practical experience, and awareness, is necessary. Professionalization and certification licensing provide a validated and recognized expert cadre of system administrators.
8. **Types of threats** - Cyber threats include denial of service, unauthorized vulnerability probes, botnet command and control, data exfiltration, data destruction or even physical destruction via alternation of critical software/data. These threats can be initiated and maintained by a mixture of malware, social engineering, or highly sophisticated advanced persistent threats (APTs) that are targeted and continue for long periods of time. The most sophisticated cyber threats are covert, do not stand out from normal activity, and are extremely difficult to detect.
9. **Advanced persistent threats -** An adversary that possesses sophisticated levels of expertise and significant resources, allowing them to create opportunities to achieve their objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

2.3 LOGICAL INTERFACE CATEGORIES

Each logical interface in the logical reference model was allocated to a logical interface category (LIC). 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 H can be used as guidelines by organizations that are developing a cybersecurity 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 ▪ (NOTE: LICs 1-4 are separate due to the architecturally significant differences between the availability and constraints, which impact mitigations such as encryption.)	U67, U79, U81, U82, U85, U102, U117, 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	U67, U79, U81, U82, U85, U102, U117, 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	U67, U79, U81, U82, U85, U102, U117, 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	U67, U79, U81, U82, U85, U102, U117, 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	U7, U9, U11, U13, U27, U65, U67, U83, U87, U115, Ux2
6. Interface between control systems in different organizations, for example: ▪ Between an RTO/ISO EMS and a utility energy management system	U10, U56, U66, U70, U74, U80, U83, U87, U89, U90, U115, U116, Ux3

Logical Interface Category	Logical Interfaces
7. Interface between back office systems under common management authority, for example: ▪ Between a Customer Information System and a Meter Data Management System	U2, U4, U21,U22, U26, U31, U53, U96, U98, U110, Ux4
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, U4, U6, U15, U52, U53, Ux4, Ux6
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: ▪ Between a Retail aggregator and an Energy Clearinghouse	U4, U9, U17, U20, U51, U52, U53, U55, U57, U58, 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, U52, 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	U2, U6, U7, U8, U21, U24, 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	U2, U6, U7, U8, U21, U24, U25, U32, U95, U119, U130

Logical Interface Category	Logical Interfaces
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
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, U42, U88, U92, 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, U101, U104, U105
18. Interface between metering equipment, for example: ▪ Between sub-meter to meter ▪ Between PEV meter and Energy Service Provider	U24, U25, U41, U46, U47, U48, U50, U54, U60, U95, U128, U129, Ux5
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	U109, U114, U135, U136, U137
21. Interface between control systems and their vendors for standard maintenance and service, for example: ▪ Between SCADA system and its vendor	U5

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	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. (NOTE: LICs 1-4 are separate due to the architecturally significant differences between the availability and constraints, which impact mitigations such as encryption.)

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 $\leq$ 60 s scan rates)
  - Low Frequency Monitoring Mode (scan/update rates in excess of 1 min)
- 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 or low availability if supporting an asset-monitoring application.
- Communications and Computational Constraints – Computational constraints are associated with cryptography requirements on the interface. Most encryption systems operate at the Application or Network layer. Physical layer encryption, however, operates directly at the physical layer interface thereby offering enhanced security. Operation at this level is, especially in the case of optical communication, very computationally intensive due to the high data throughput and cryptography requirements. Most physical layer encryption devices therefore make use of field-programmable gate arrays (FPGAs) or other custom hardware devices to meet those needs. Existing devices like RTUs, substation IEDs, meters, and others are typically not equipped with sufficient digital hardware to perform this type of cryptographic function. Communication is also constrained to point-to-point in case of optical/cable/radio networks and point-to-multipoint in care of radio networks when physical layer encryption is applied.
- 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.

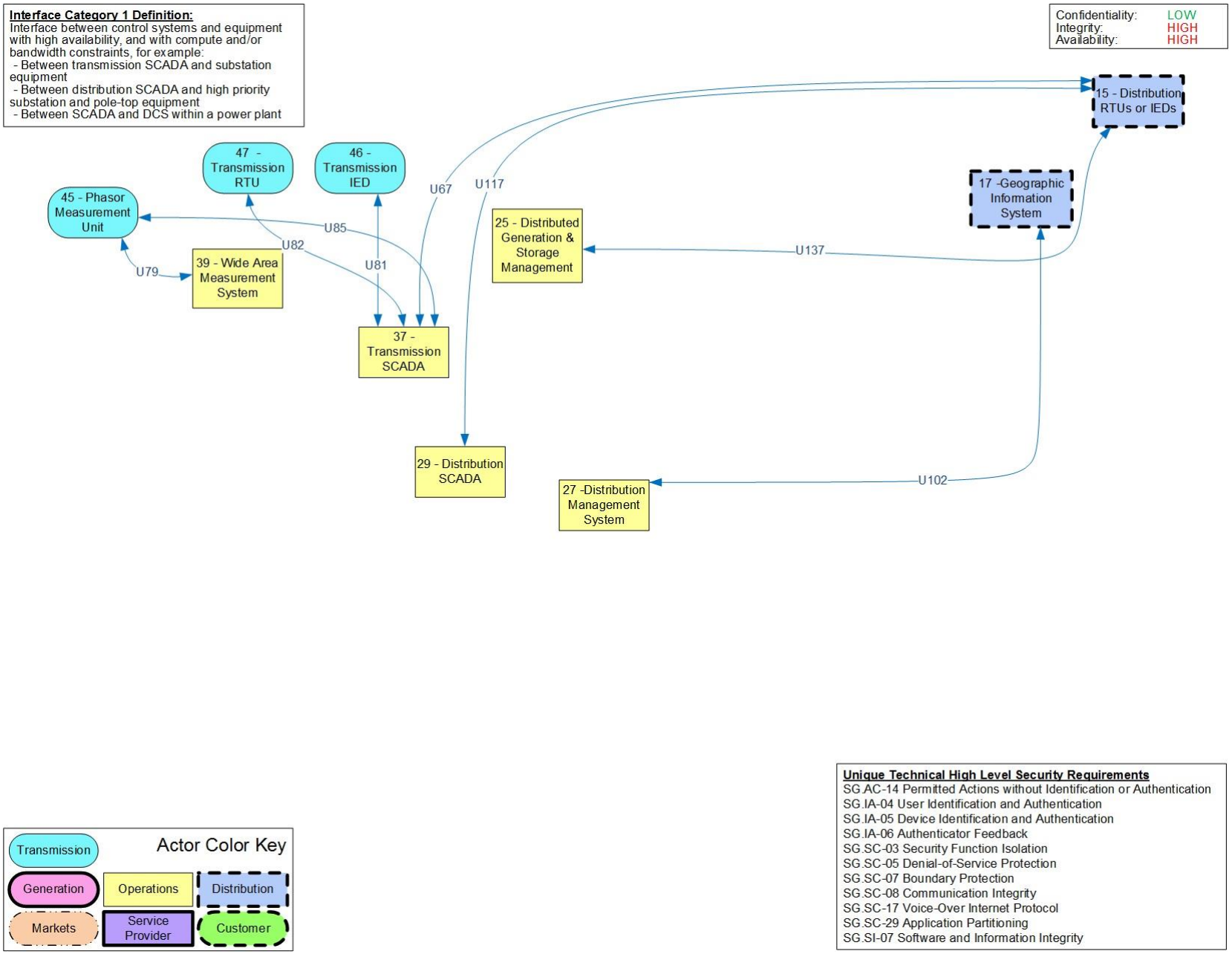


Figure 2-5 Logical Interface Category 1

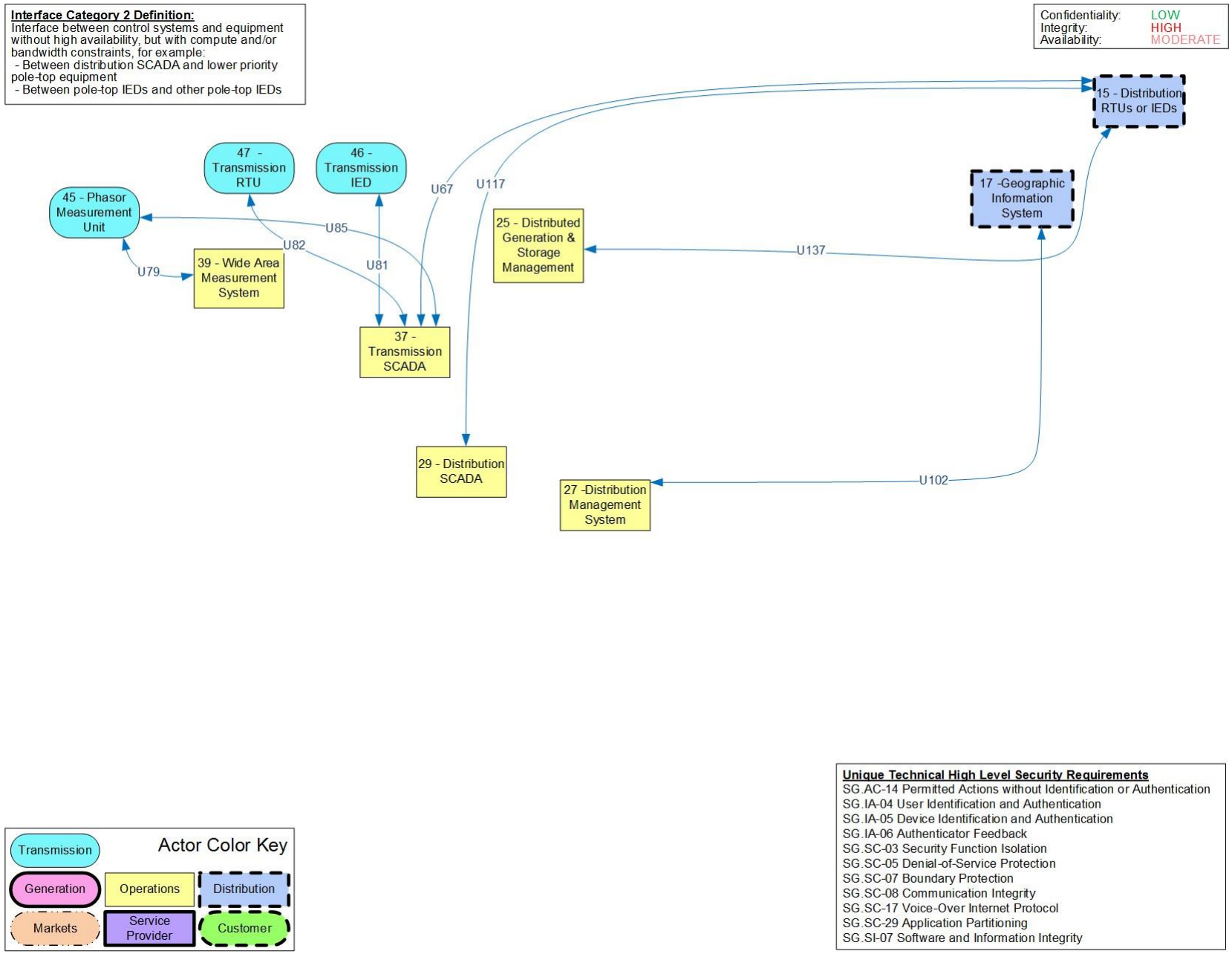


Figure 2-6 Logical Interface Category 2

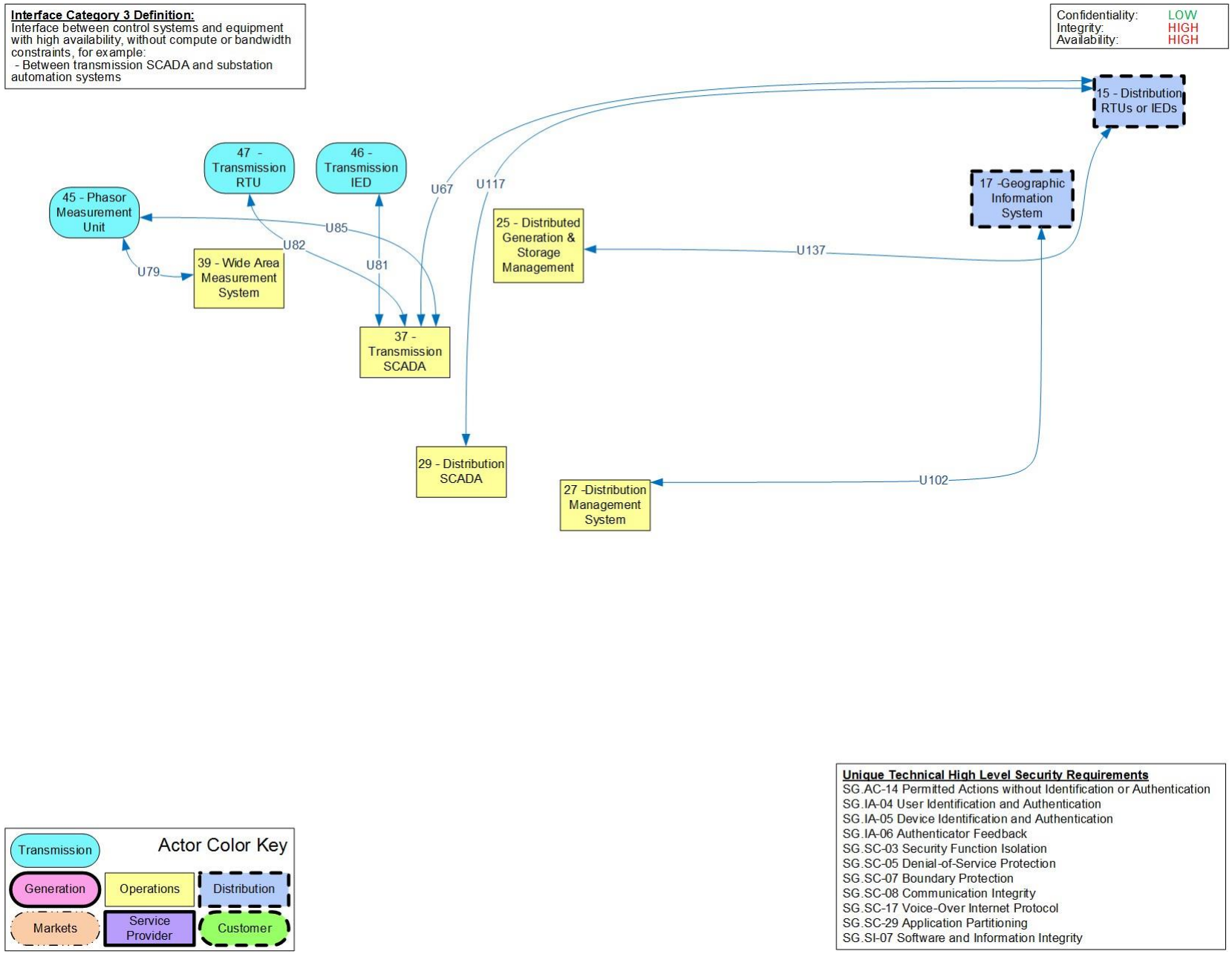


Figure 2-7 Logical Interface Category 3

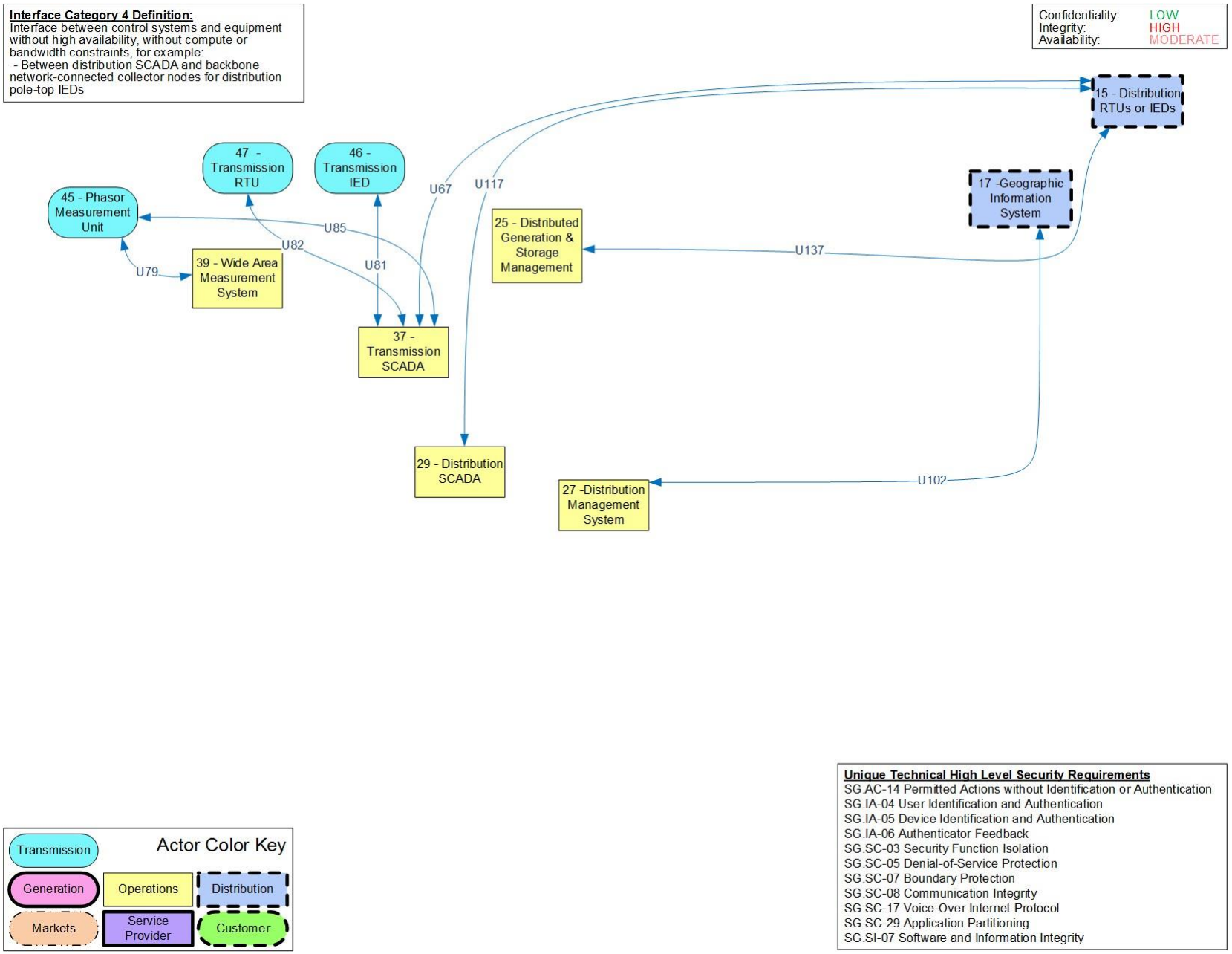


Figure 2-8 Logical Interface Category 4

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.

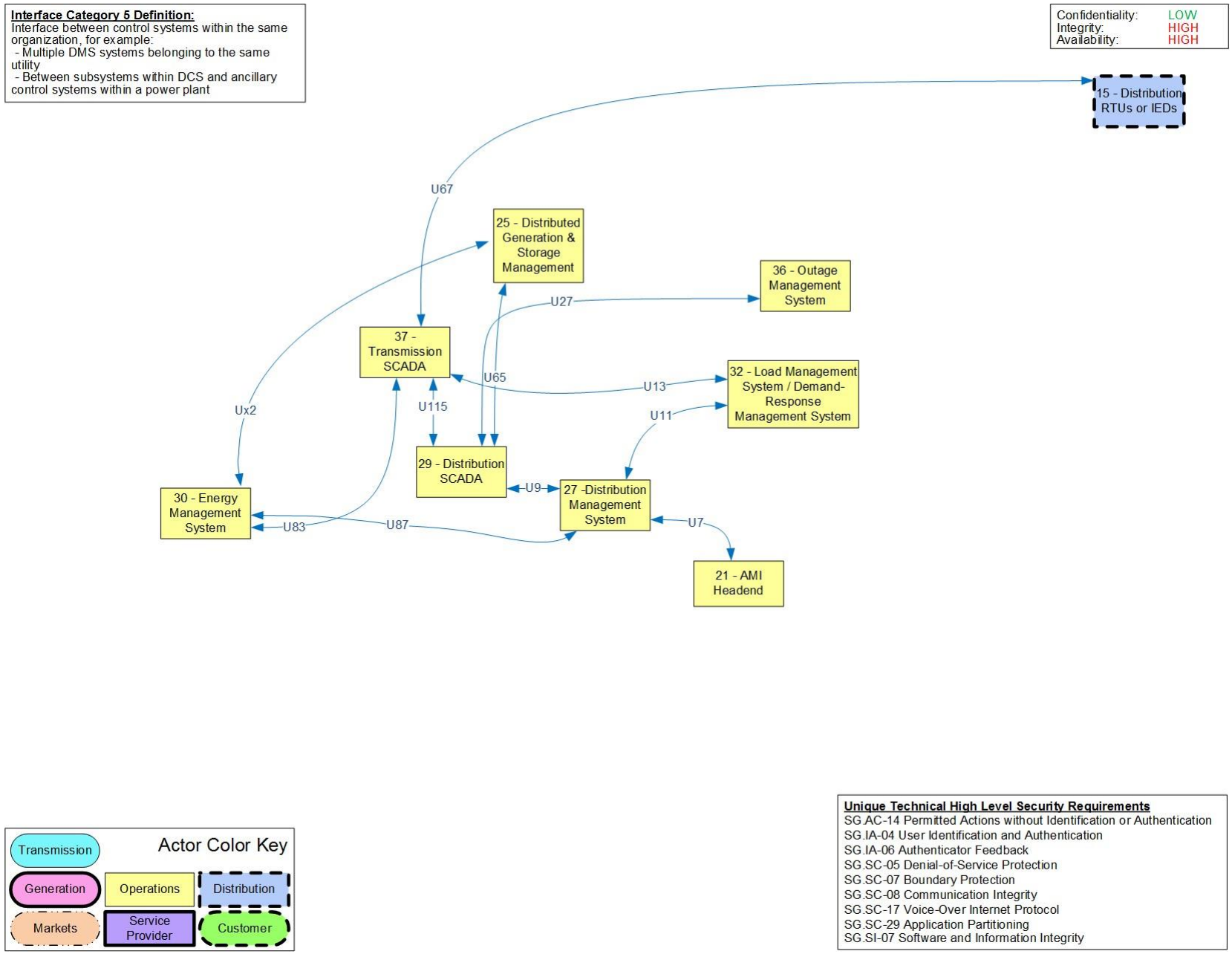


Figure 2-9 Logical Interface Category 5

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:

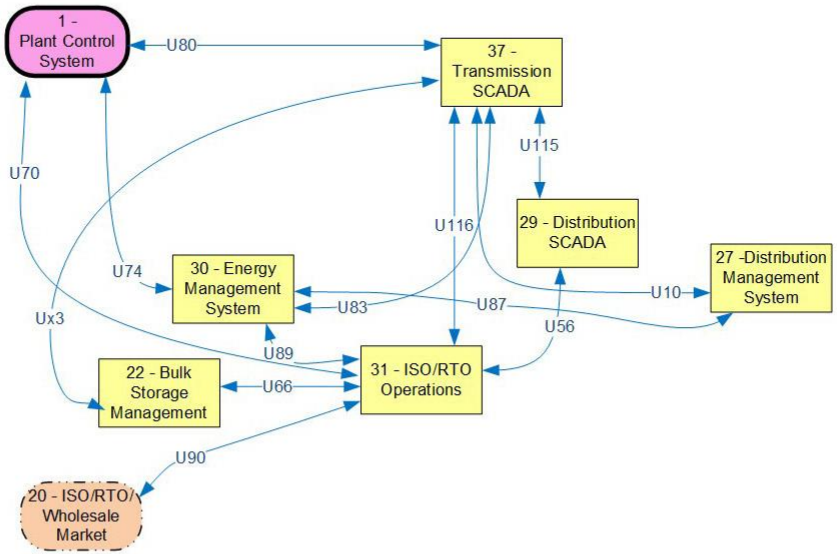
- Between an RTO/ISO EMS and a utility energy management system;
- Between a Generation and Transmission SCADA and a distribution CO-OP SCADA;
- Between a transmission EMS and a distribution DMS in different utilities; and
- Between an EMS/SCADA and a power plant DCS.

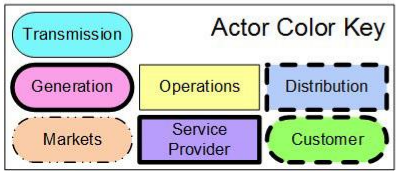
Control systems with interfaces between them have the following characteristics and issues:

- 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.

Interface Category 6 Definition:
Interface between control systems in different organizations, for example:
- Between an RTO/ISO EMS and a utility energy management system

Confidentiality: LOW
Integrity: HIGH
Availability: MODERATE





Unique Technical High Level Security Requirements
SG.AC-14 Permitted Actions without Identification or Authentication
SG.IA-04 User Identification and Authentication
SG.IA-06 Authenticator Feedback
SG.SC-05 Denial-of-Service Protection
SG.SC-07 Boundary Protection
SG.SC-08 Communication Integrity
SG.SC-17 Voice-Over Internet Protocol
SG.SC-29 Application Partitioning
SG.SI-07 Software and Information Integrity

Figure 2-10 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.

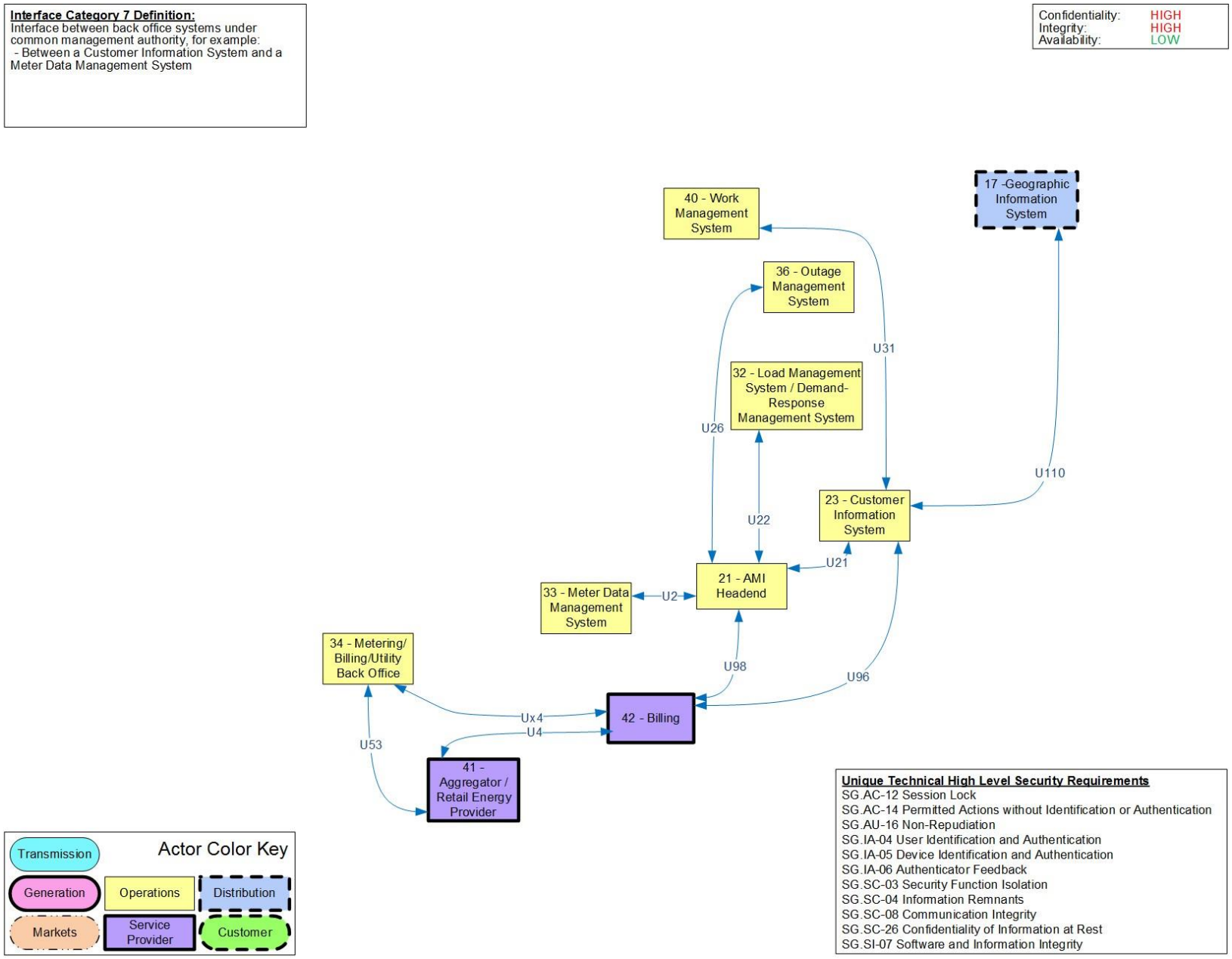
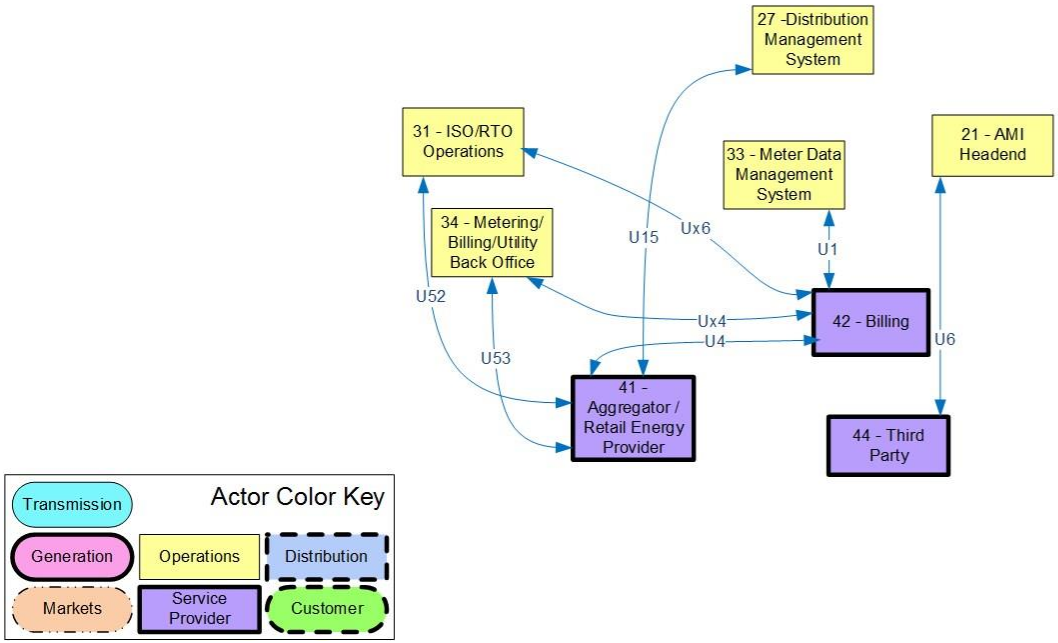


Figure 2-11 Logical Interface Category 7

Interface Category 8 Definition:
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 or an Aggregator/ Retail Energy Provider

Confidentiality:	HIGH
Integrity:	HIGH
Availability:	LOW



Unique Technical High Level Security Requirements
SG.AC-12 Session Lock
SG.AC-14 Permitted Actions without Identification or Authentication
SG.AU-16 Non-Repudiation
SG.IA-04 User Identification and Authentication
SG.IA-05 Device Identification and Authentication
SG.IA-06 Authenticator Feedback
SG.SC-03 Security Function Isolation
SG.SC-04 Information Remnants
SG.SC-07 Boundary Protection
SG.SC-08 Communication Integrity
SG.SC-26 Confidentiality of Information at Rest
SG.SI-07 Software and Information Integrity

Figure 2-12 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.[29]
- 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, low 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.
- 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.

[29] For more on what privacy and confidentiality are, please see Vol. 2, §5.2 What is Privacy?

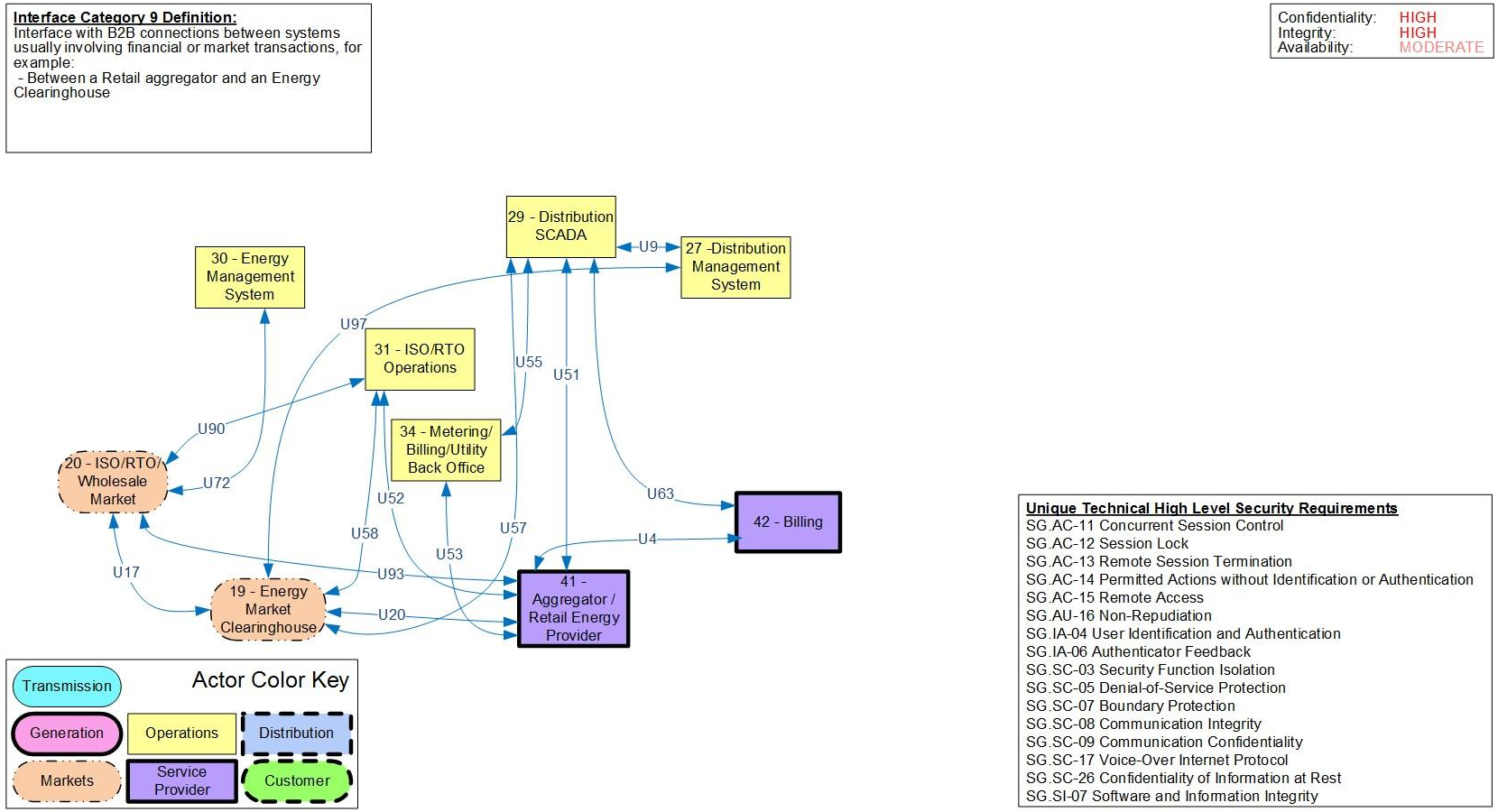


Figure 2-13 Logical Interface Category 9

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 head-end 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 availability 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.

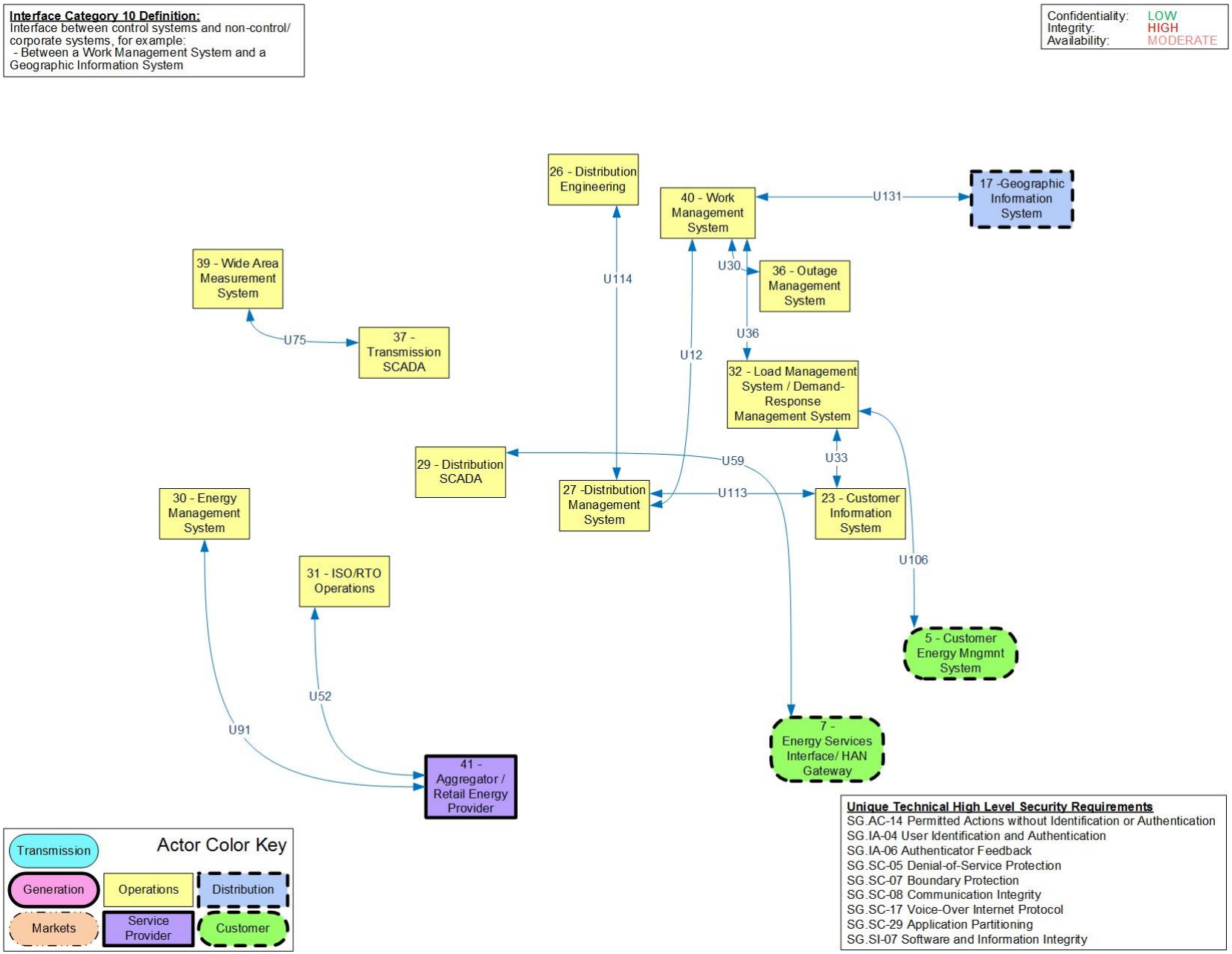


Figure 2-14 Logical Interface Category 10

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.

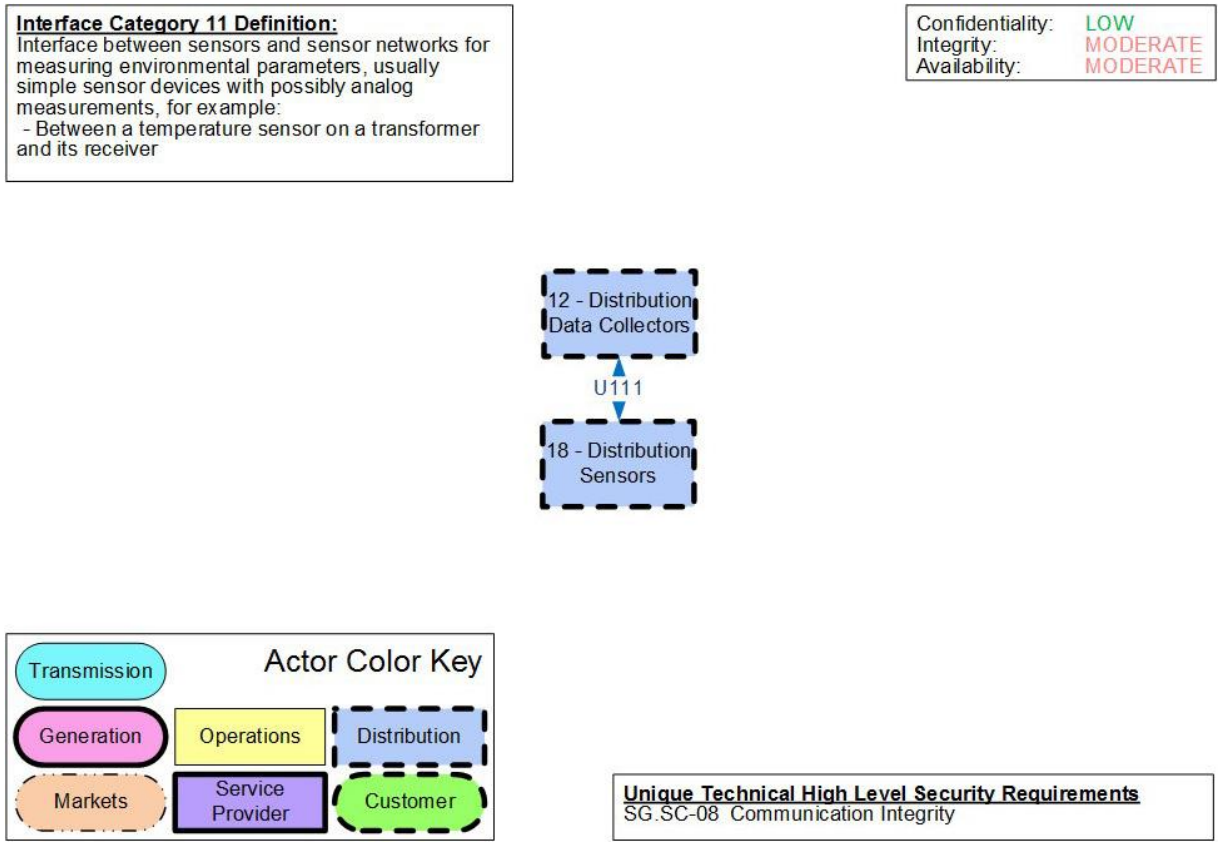


Figure 2-15 Logical Interface Category 11

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.

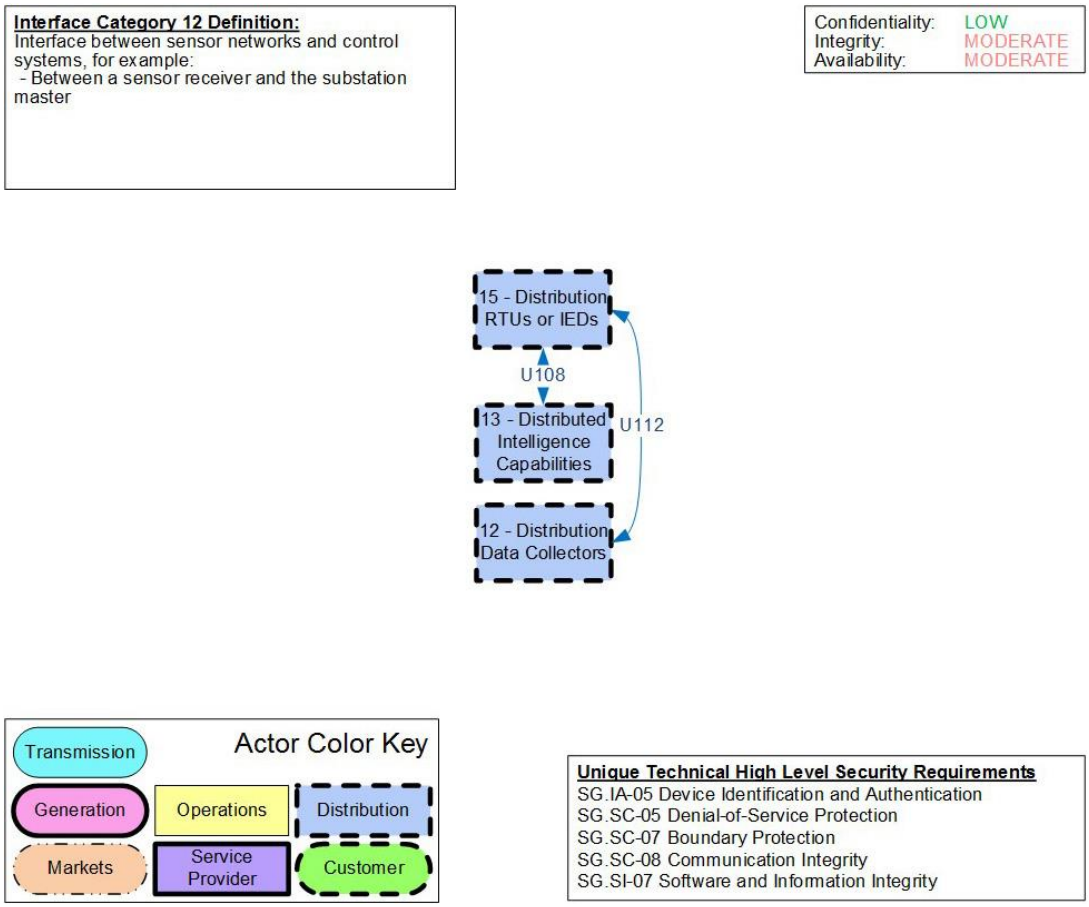


Figure 2-16 Logical Interface Category 12

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:

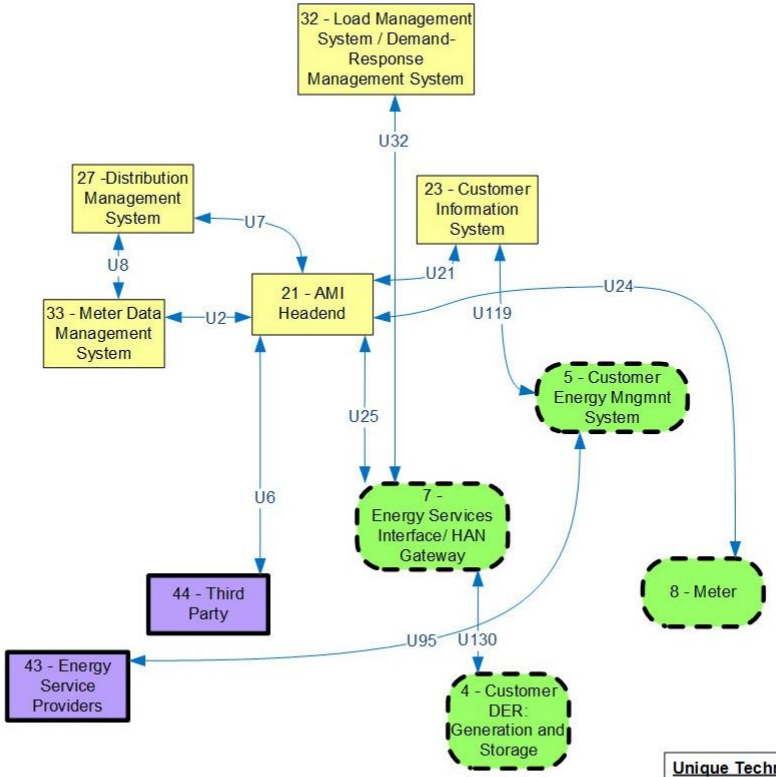
- Between MDMS and meters; and
- Between LMS/DRMS and Customer EMS.

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 connect a utility, which has corporate security requirements, with customers, that have 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.

Interface Category 13 Definition:
Interface between systems that use the AMI network, for example:
- Between MDMS and meters
- Between LMS/DRMS and Customer EMS

Confidentiality: HIGH
Integrity: HIGH
Availability: LOW



Unique Technical High Level Security Requirements
SG.AC-14 Permitted Actions without Identification or Authentication
SG.AU-16 Non-Repudiation
SG.IA-04 User Identification and Authentication
SG.IA-06 Authenticator Feedback
SG.SC-03 Security Function Isolation
SG.SC-04 Information Remnants
SG.SC-07 Boundary Protection
SG.SC-08 Communication Integrity
SG.SC-09 Communication Confidentiality
SG.SC-26 Confidentiality of Information at Rest
SG.SC-29 Application Partitioning
SG.SI-07 Software and Information Integrity

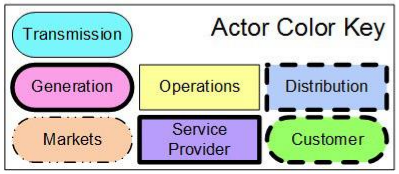


Figure 2-17 Logical Interface Category 13

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:

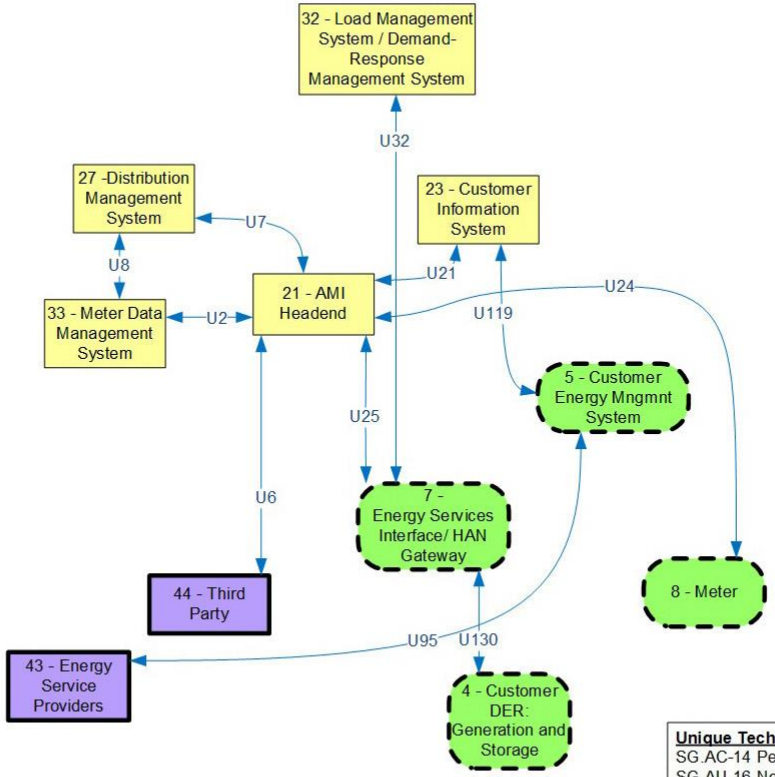
- Between LMS/DRMS and customer DER;
- Between DMS applications and customer DER; and
- Between DMS applications and distribution automation (DA) field equipment.

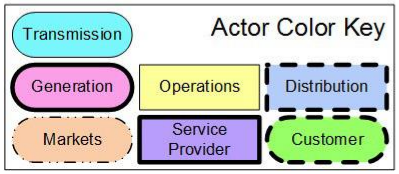
Although both logical interface categories 13 and 14 use the AMI network to connect to field sites, the issues for logical interface category 14 differ from those of 13, because the interactions are focused on power operations of DER and DA equipment. Therefore the issues include the following:

- 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 connect a utility, which has corporate security requirements, with customers, that have 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.

Interface Category 14 Definition:
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

Confidentiality: HIGH
Integrity: HIGH
Availability: HIGH





Unique Technical High Level Security Requirements
SG.AC-14 Permitted Actions without Identification or Authentication
SG.AU-16 Non-Repudiation
SG.IA-04 User Identification and Authentication
SG.IA-06 Authenticator Feedback
SG.SC-03 Security Function Isolation
SG.SC-04 Information Remnants
SG.SC-05 Denial-of-Service Protection
SG.SC-07 Boundary Protection
SG.SC-08 Communication Integrity
SG.SC-09 Communication Confidentiality
SG.SC-17 Voice-Over Internet Protocol
SG.SC-26 Confidentiality of Information at Rest
SG.SC-29 Application Partitioning
SG.SI-07 Software and Information Integrity

Figure 2-18 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.

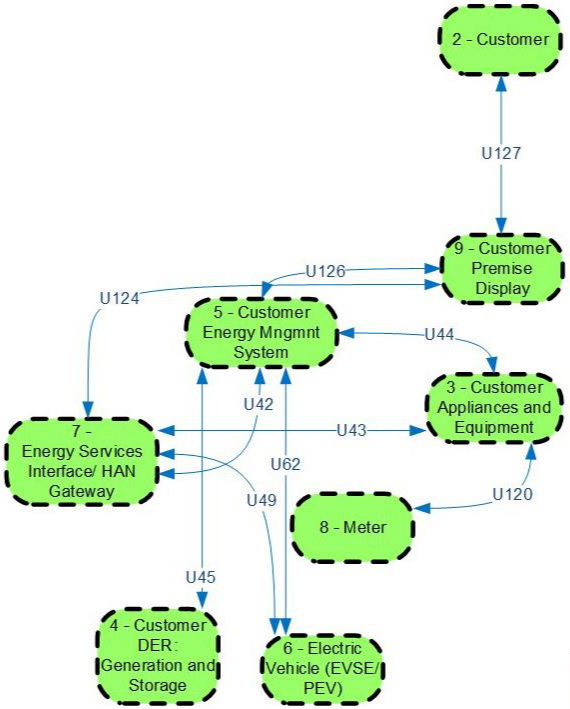
The security-related issues for this intra-customer site environment HAN/BAN/NAN interface category include the following:

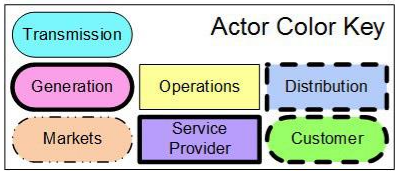
- Some information exchanged among different appliances and systems must be treated as confidential to ensure that an unauthorized third party does not gain access to it. For instance, energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential.
- 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.

Interface Category 15 Definition:
Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs, for example:
- Between Customer EMS and Customer Appliances
- Between Customer EMS and Customer DER
Between Energy Service Interface and PEV

Confidentiality: LOW
Integrity: MODERATE
Availability: MODERATE





Unique Technical High Level Security Requirements
SG.AC-12 Session Lock
SG.AC-13 Remote Session Termination
SG.AC-14 Permitted Actions without Identification or Authentication
SG.AC-15 Remote Access
SG.IA-04 User Identification and Authentication
SG.IA-05 Device Identification and Authentication
SG.IA-06 Authenticator Feedback
SG.SC-03 Security Function Isolation
SG.SC-05 Denial-of-Service Protection
SG.SC-07 Boundary Protection
SG.SC-08 Communication Integrity
SG.SC-09 Communication Confidentiality
SG.SC-17 Voice-Over Internet Protocol
SG.SC-26 Confidentiality of Information at Rest
SG.SI-07 Software and Information Integrity

Figure 2-19 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 should 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 should be kept confidential.
- 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.

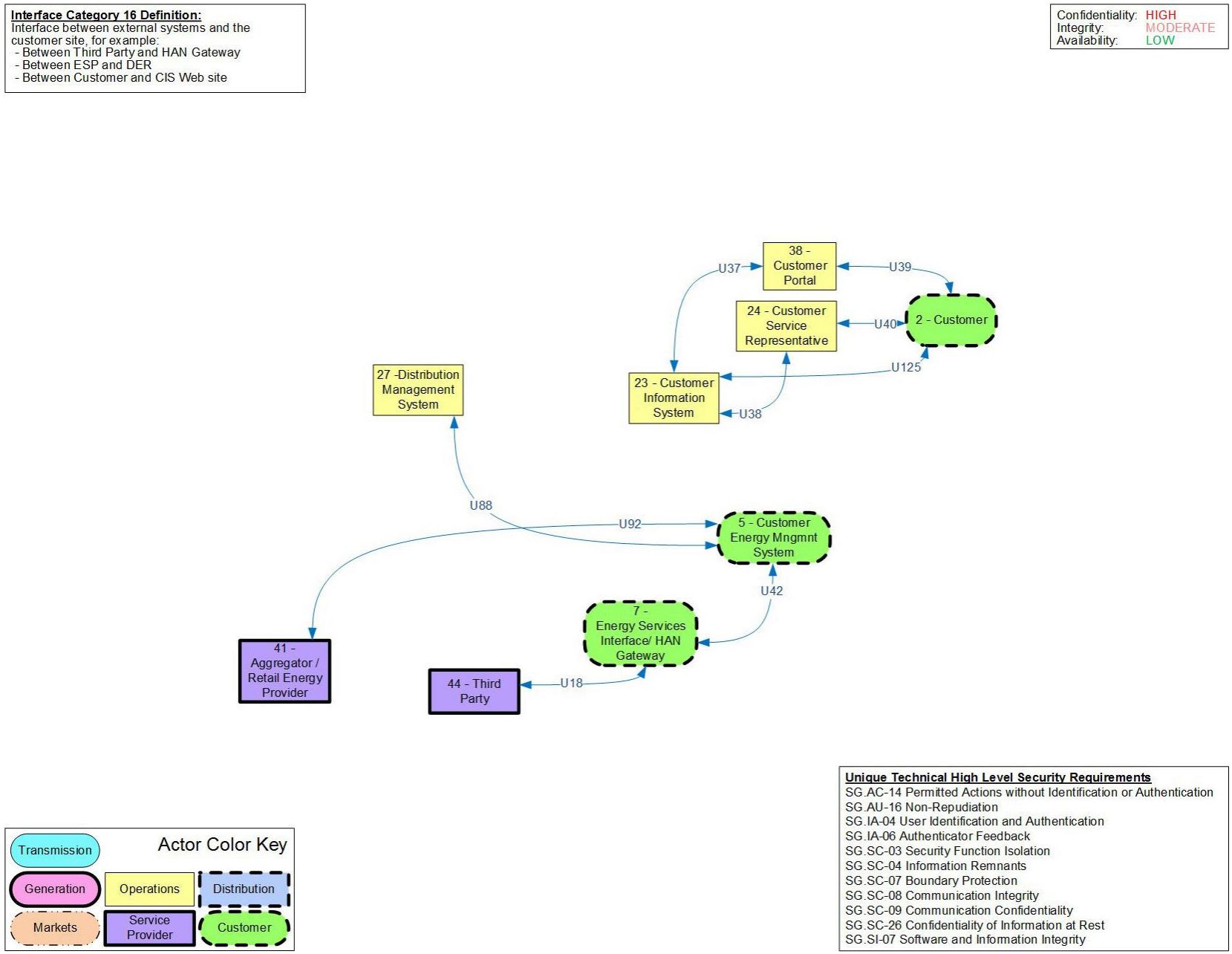


Figure 2-20 Logical Interface Category 16

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 other mobile devices (such as smart phones or tablets) 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
- Dynamic discovery of markets, dynamic entry into markets, and dynamic exit from markets.

The key characteristics of this interface category are as follows:

- This interface is primarily for customer-side service operations. The most critical needs for this interface are
  - To post restoration information back to the OMS for prediction 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 other mobile devices 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/mobile device until it is reconnected to a physical network.
- Note: Data that is captured (e.g., metering data, local device passwords, security parameters) should be protected at the appropriate level.

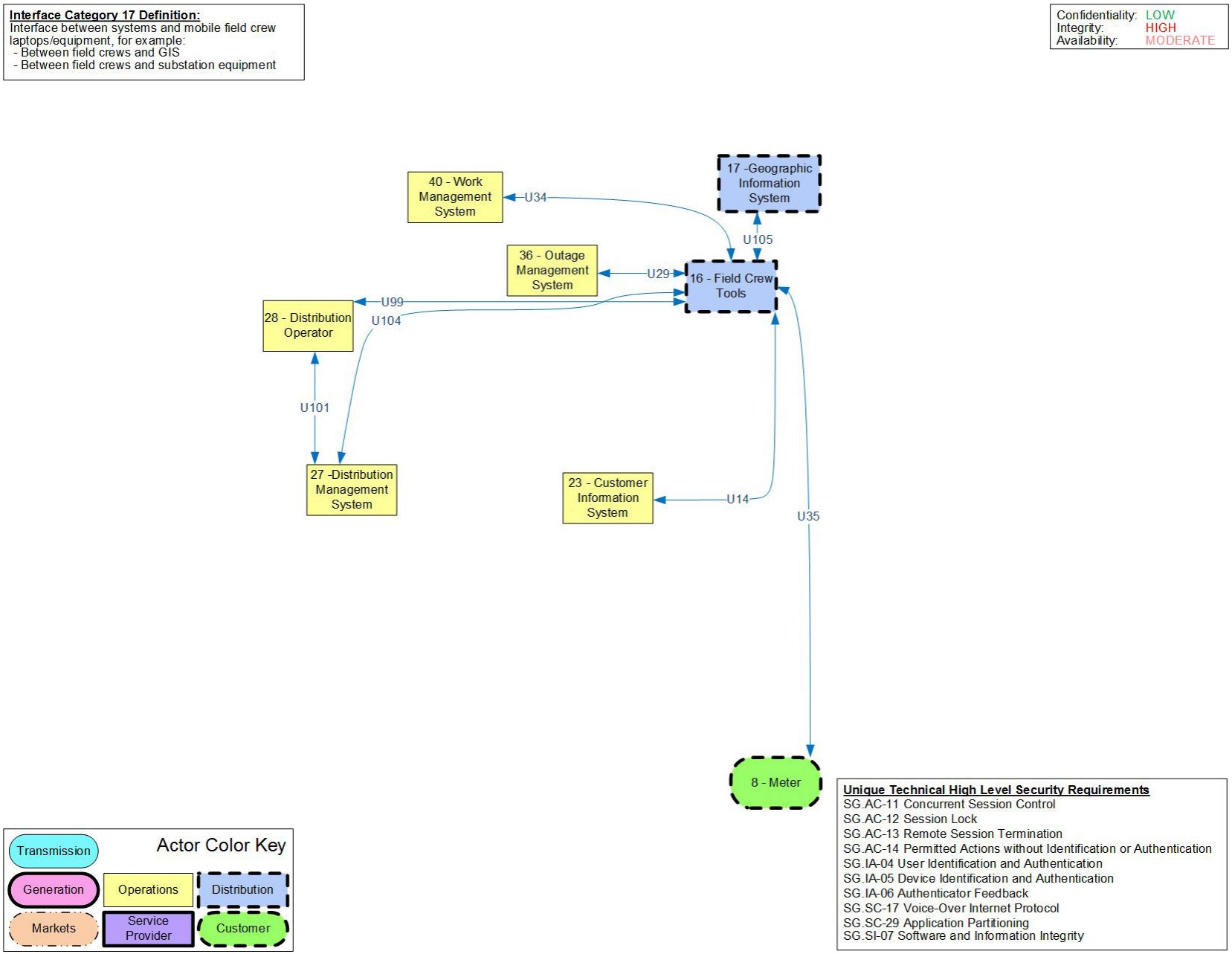


Figure 2-21 Logical Interface Category 17

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.

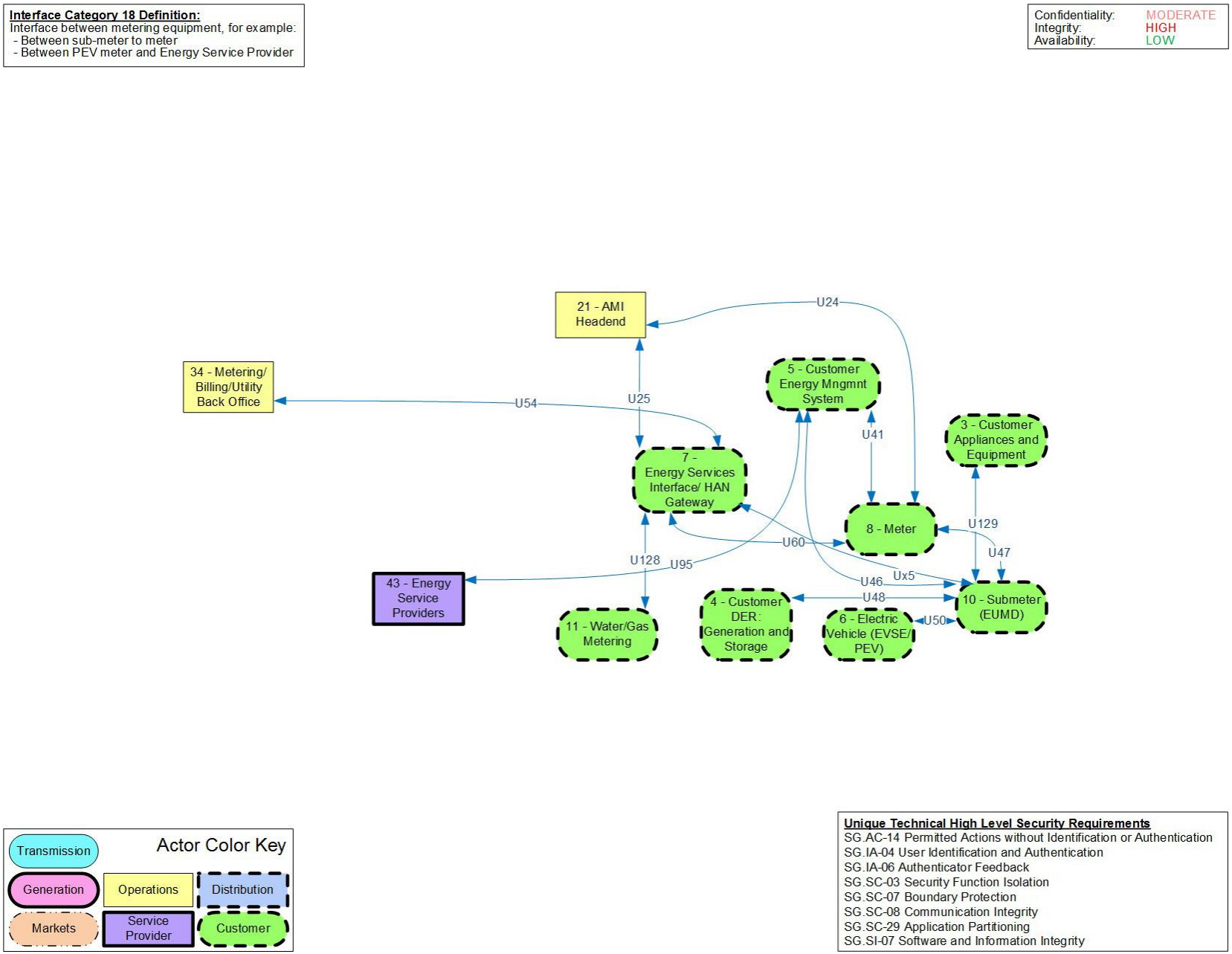


Figure 2-22 Logical Interface Category 18

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). Some interactions across interfaces should be treated as critical infrastructure information requiring confidentiality in order to avoid unauthorized persons from using the information to plan an attack. Other information is not confidential at all. If it is determined that confidentiality is needed, then appropriate requirements should be put in place.

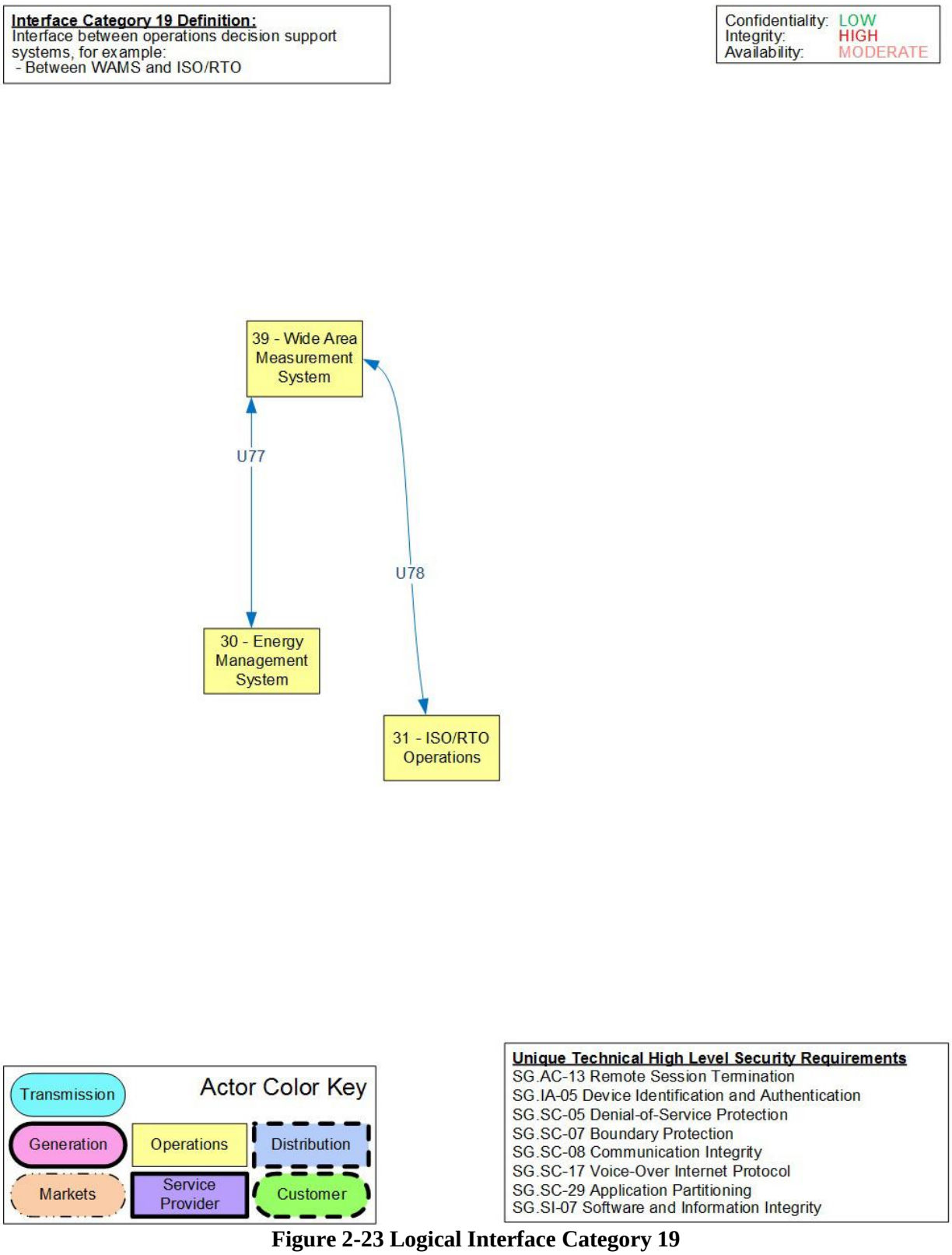


Figure 2-23 Logical Interface Category 19

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
- Updating software.

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.
- Some device settings should be treated as critical infrastructure information requiring confidentiality in order to avoid unauthorized persons from using the settings to plan an attack. Other settings are not confidential at all. If it is determined that confidentiality is needed, then appropriate requirements should be put in place.
- 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.

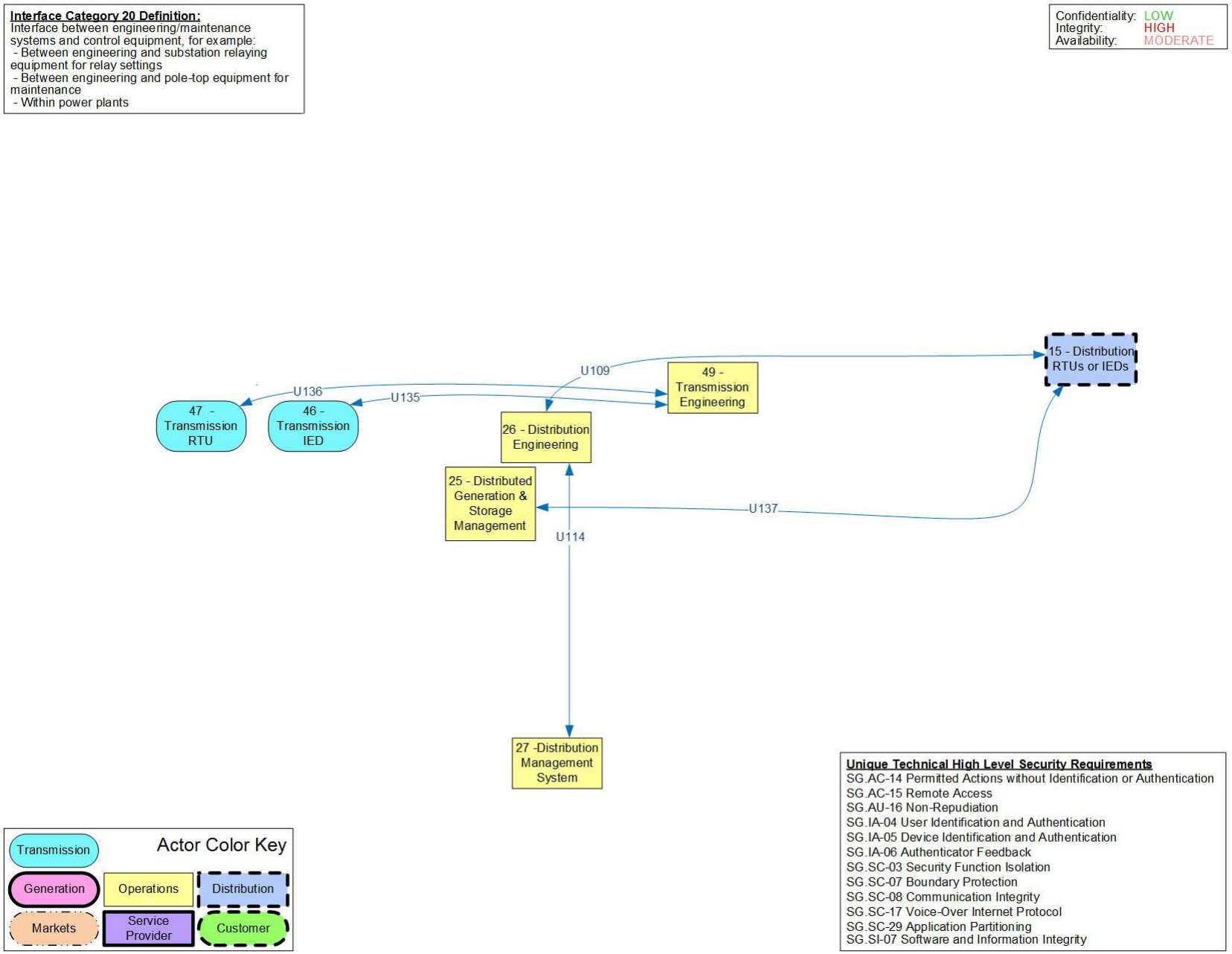


Figure 2-24 Logical Interface Category 20

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 to perform troubleshooting and problem resolution (see Logical Interface Categories 1-4, 5-6, or 20, depending upon the role).

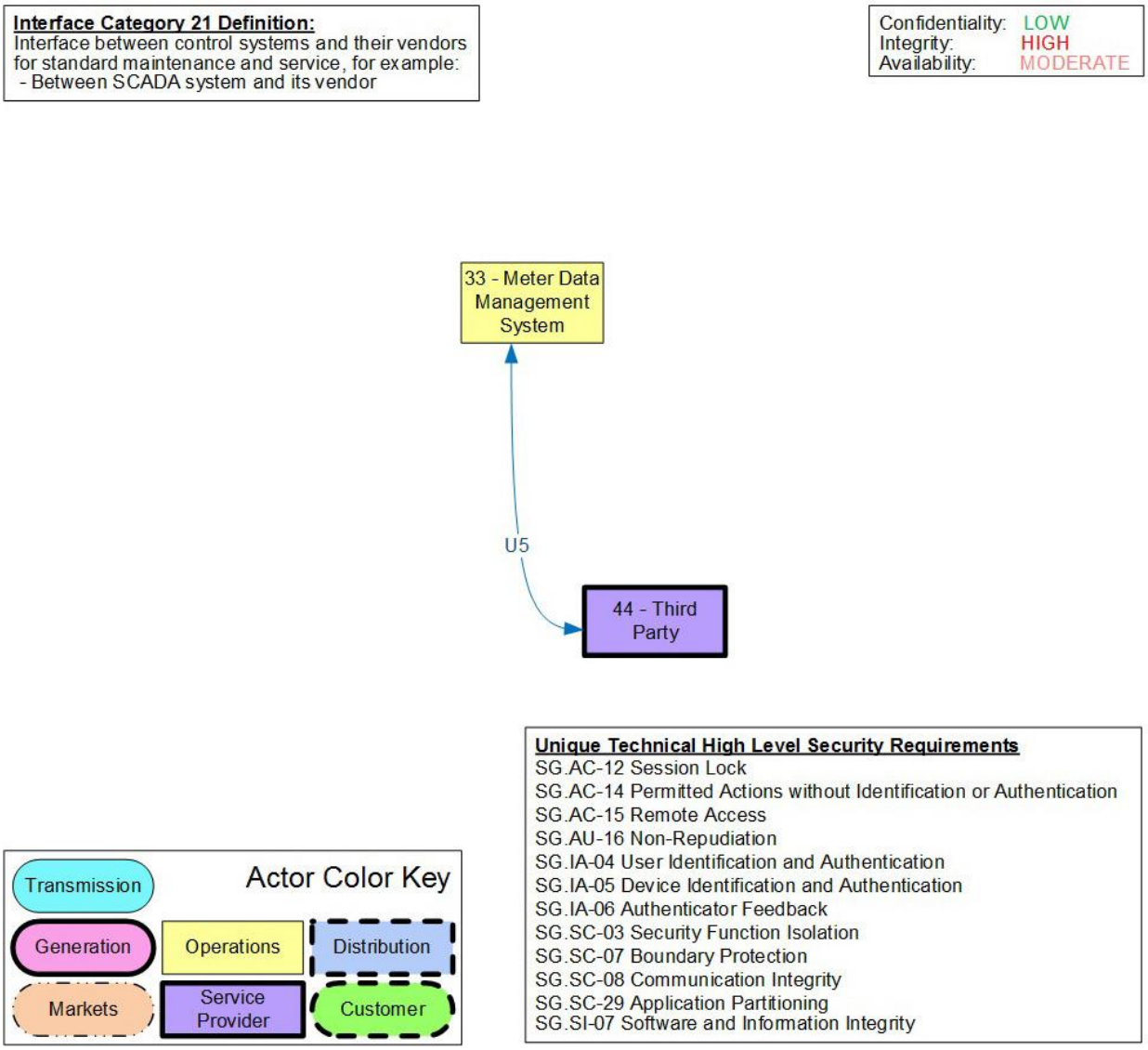


Figure 2-25 Logical Interface Category 21

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.)

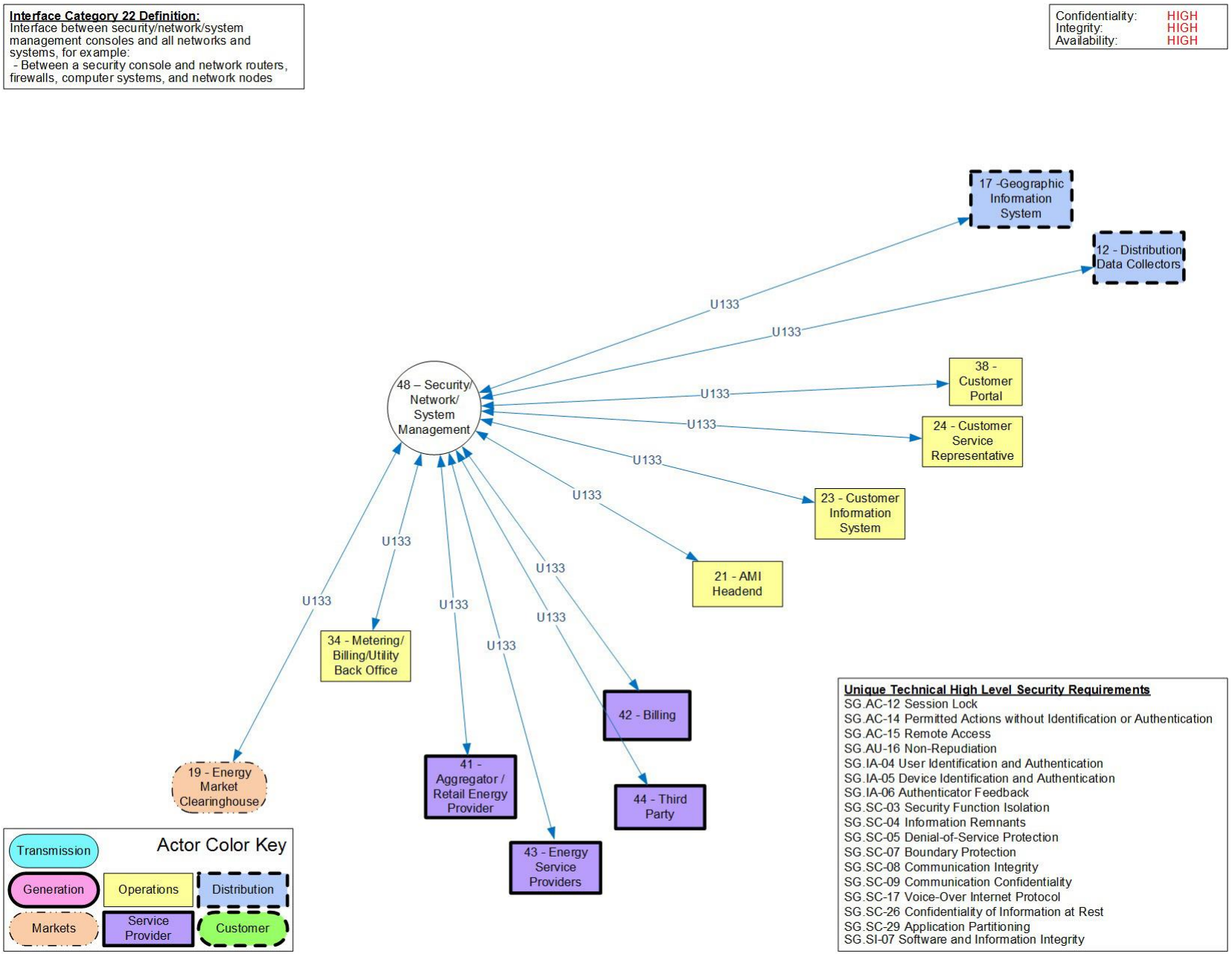


Figure 2-26 Logical Interface Category 22

CHAPTER 3
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 H. 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 CYBERSECURITY 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/days 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 US 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.	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.	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.	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 cybersecurity 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 cybersecurity 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	H	L
8	H	H	L
9	H	H	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	M	H	L
19	L	H	M
20	L	H	M
21	L	H	M
22	H	H	H

3.4 SELECTION OF SECURITY REQUIREMENTS

Power system operations pose many security challenges that are different from most other industries. In many cases, legacy equipment in industrial control systems that are in use in the power system operations may not be able to incorporate all requirements in this document, yet still need the protections offered by the requirements. 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.
- Power system management, monitoring, and control will increasingly extend away from the power entities' traditional physical and security environments into external environments that the power entity has little or no influence and control over.

There is no single set of cybersecurity requirements that addresses each of the smart grid logical interface categories. This information can be used as guidelines for organizations as they develop their cybersecurity strategy, perform risk assessments, and select and modify security requirements for smart grid information system implementations.

Additional criteria must be used in determining the cybersecurity requirements before selecting and implementing the cybersecurity 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 cybersecurity requirements can be applied that are both specific enough to be applicable to the interfaces and general enough to permit the implementation of different cybersecurity solutions that meet the security requirements or embrace new security technologies as they are developed. This cybersecurity 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.[30] 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. GRC requirements, while centered around policy,

[30] Full references to these documents are in §1.3 Smart Grid Cybersecurity Document Development Strategy, Task 3.

procedure, and compliance-based activities, may include technical implications. It may be necessary to augment these organization-level requirements for different types of organizational security structures, 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 that 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]) in Table 3-3. 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 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.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-11									H								H					
SG.AC-12							H	H	M						M		M				M	H
SG.AC-13									M						M		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						M					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																					

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-1	Applies at all impact levels																					
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																					

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.AU-15	Applies at all impact levels																				
SG.AU-16							H	H	H				H	H		H				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																				

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-1	Applies at all impact levels																					
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 all impact levels with additional requirement enhancements 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 level																					
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			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

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-1	Applies at all impact levels																					
SG.ID-2	Applies at all impact levels																					
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																					

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-5	Applies at all impact levels																					
SG.MA-6	Applies at all impact levels with additional requirement enhancements at high impact levels																					
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																					

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.PE-12	Applies at all impact levels with additional requirement enhancements at high impact level																					
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 moderate and high 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																					

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-6	Applies at all impact levels																					
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	H	M	M		H		H	H	H
SG.SC-4							H	H					H	H		H						H
SG.SC-5	H	M	H	M	M	M			M	M		M		H	M				M			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	M	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-17	H	M	H	M	H	M			M	M				H	M		M		M	M		H
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	M	H						H

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.SC-29	H	H	H	H	H	H				H			H	H			H	H	H	H	H	H
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																					

2

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.

Organizations should leverage this volume of NISTIR as they implement their cybersecurity strategy and perform risk assessments.[31]

After performing a risk assessment, an organization should select the appropriate set of cybersecurity requirements applicable to the selected logical interface category. These security requirements, including GRCs, common technical and unique technical, could then be tailored to

[31] For additional information on conducting a risk assessment, refer to NIST Special Publication 800-30, Rev. 1, *Guide for Conducting Risk Assessments*, Sep. 2012, available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

meet the specific risk criteria and smart grid information system functional and performance requirements, technical characteristics, and security vulnerabilities. Not all security requirements are assigned to impact levels, as indicated by the phrase "Not Selected." In those cases, the security requirements should be applied as appropriate.

After the selection of the initial set of security requirements, the selected requirements should be tailored to ensure they are appropriately modified and closely aligned to address the conditions for the smart grid information system. This tailoring process includes:

- Selecting the appropriate security requirements, including GRCs, common technical, and unique technical;
- Identifying aspects of the selected security requirements that would need modifications or clarifications to apply to the smart grid information system;
- Identifying security policy issues in the GRCs to ensure they are covered in the appropriate security policies in the organization;
- Identifying how the common technical and unique technical requirements are or would be address in the smart grid information system design and implementation;
- Identifying security gaps where compensating security requirements or measures are needed; ensuring the compensating security requirements or measures meet the security goals of the organization; and
- Specifying, as appropriate, which security requirements should be met for different stakeholders of the smart grid information system (vendors, implementers, operations, maintenance, users, etc.).

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[32] are important requirements for safety. These are outside the scope of cybersecurity and are not included in this report. However, these requirements should 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 §5.13, 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.

[32] 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.

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:

1. Authorizing, establishing, activating, modifying, disabling, and removing accounts;
2. Specifying account types, access rights, and privileges (e.g., individual, group, system, guest, anonymous and temporary);
3. Reviewing accounts on an organization-defined frequency; and
4. Notifying account managers when smart grid information system users are terminated, transferred, or smart grid information system usage changes.
5. Requiring management approval 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 organization requires smart grid information systems to enforce 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 Governance, Risk, and Compliance (GRC) Requirements

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 Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Assigns the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks; and
2. 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

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

Logging both unsuccessful and successful login attempts can be of use for auditing purposes. 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 should 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

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. 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, Availability

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. The scope of this requirement is only for users who log into systems where the login impacts performance. This does not include the login into devices, which may require additional session control.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

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

SG.AC-12 Session Lock

Category: Unique Technical Requirements

Requirement

The smart grid information system—

1. Prevents further access 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

The organization—

1. Identifies and documents specific user actions, if any, that can be performed on the smart grid information system without identification or authentication; and

2. Identifies 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 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 Governance, Risk, and Compliance (GRC) Requirements

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 Governance, Risk, and Compliance (GRC) Requirements

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 Technical Requirements

Requirement

Smart grid information systems are designed and implemented with mechanisms to restrict access between the smart grid information system and 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 Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Develops and enforces policies and procedures for smart grid information system users concerning the generation and use of passwords;
2. Stipulates rules of complexity, based on the criticality level of the smart grid information system to be accessed; and
3. Requires passwords to be changed regularly and be revoked after an extended period of inactivity.

Supplemental Guidance

NIST Special Publication 800-63-2, *Electronic Authentication Guideline,* Appendix A, provides additional guidance on passwords.

Requirement Enhancements

None.

Additional Considerations

A1. Password complexity tools are used to ensure conformity with password policy.

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

The organization—

1. 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. 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. Ensures security responsibility is 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 its 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 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. With the convergence of power systems and traditional IT systems, proper analysis of event information is necessary in order to understand what occurred during the event. This analysis should acknowledge both disciplines, as organizations will benefit from joint analysis of events. For example, analysis teams need to evaluate power systems logging data and cyber event logs in order to properly ascertain the actual causes of an event.

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 Governance, Risk, and Compliance (GRC) Requirements

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

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 Governance, Risk, and Compliance (GRC) Requirements

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 Technical 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 Analysis Tools and Report Generation

Category: Common Technical Requirements

Requirement

The smart grid information system provides audit analysis tools and report generation capability.

Supplemental Guidance

Audit analysis tools allow collected audit information to be manipulated and organized into a summary format that may be meaningful to analysts. Audit analysis tools 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 Technical 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, accurate 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 Technical 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 cybersecurity 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 cybersecurity 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 Record Generation

Category: Common Technical Requirements

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 consolidate audit records from multiple components into a 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. Additionally, the organization develops procedures to preserve data during update actions to ensure continuity of operations and in case updates need to be "rolled back."

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

Requirement

The smart grid information system—

1. Is configured 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. Is reviewed 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 Governance, Risk, and Compliance (GRC) Requirements

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). The component inventory may also include a network diagram.

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 should 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 Technical Requirements

Requirement

The smart grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other 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 should 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

The organization develops and reviews the policies and procedures detailing the handling of information 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 Technical 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

A1. 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

The organization—

1. Develops and implements policies and procedures include an incident response investigation and analysis program;
2. Includes investigation and analysis of smart grid information system incidents in the planning process; and
3. 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

The organization—

1. Reviews investigation results and determines corrective actions needed; and
2. Includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of cybersecurity 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 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 cybersecurity 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

1. The organization 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. The organization 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 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

1. 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. 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

1. 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 Technical Requirements

Requirement

Emergency power-off capability is protected 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 Technical Requirements

Requirement

An alternate power supply is available 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

The organization—

1. 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. 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 cybersecurity policy, assign security roles, and coordinate the implementation of cybersecurity 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—

1. Assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions;
2. Reviews and revises position risk designations; and
3. 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—

1. Screens individuals requiring access to the smart grid information system before access is authorized; and
2. 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

The organization—

1. Revokes logical and physical access to facilities and systems and ensures that all organization-owned property is returned when an employee is terminated. 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. Terminates all logical and physical access on an organization-defined time frame for personnel terminated for cause; and
3. Conducts exit interviews to 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

The organization—

1. 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. Reviews and updates access agreements periodically; and
3. Ensures that 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

The organization—

1. 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. 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. 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

The organization—

1. Ensures 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. 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

The organization—

1. Requires the smart grid information system documentation to include how to configure, install, and use the smart grid information system and its security features; and
2. 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 those 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 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 Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization requires —

1. The smart grid information system developer to create a security test and evaluation plan;
2. The developer to submit the plan to the organization for approval and implement the plan once written approval is obtained;
3. The developer document the results of the testing and evaluation and submit them to the organization for approval; and
4. Developmental security tests not be performed 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 Governance, Risk, and Compliance (GRC) Requirements

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

Security functions are the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

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. For example, the operating system reallocates storage without completely deleting the previous data.

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, demilitarized zones (DMZ) 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 should be restricted to specific components in the smart grid information system. Communications should 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, Integrity

Requirement

The smart grid information system protects the integrity of electronically communicated information.

Supplemental Guidance

It is feasible to implement this requirement at one or more various locations within the communications stack; each placement location carries varying benefits and downsides.

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, Confidentiality

Requirement

The smart grid information system protects the confidentiality of communicated information.

Supplemental Guidance

It is feasible to implement this requirement at one or more various locations within the communications stack; each placement location carries varying benefits and downsides.

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

Requirement

The smart grid information system employs secure methods for the establishment and management of cryptographic keys.

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 NIST Approved Cryptography

Category: Common Technical Requirements

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 should 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 4 Cryptography and Key Management.

Requirement Enhancements

None.

Additional Considerations

A1. The organization ensures that vendors have validated or demonstrated conformance of their cryptographic modules and other security functions.

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

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

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

Requirement

All external smart grid information system and communication connections are identified and protected from tampering or damage.

Supplemental Guidance

The intent of this requirement is to address end-to-end connection integrity. For example, 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). This requirement applies to dedicated connections between smart grid information systems and does not apply to transitory, user-controlled connections.

Requirement Enhancements

None.

Additional Considerations

A1. Logical connections are monitored for changes in configured or remote endpoints.

Impact Level Allocation

Low: SG.SC-18	Moderate: SG.SC-18	High: SG.SC-18

SG.SC-19 Security Roles

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

Requirement

The organization designs and specifies the implementation of security roles and responsibilities for the users of the smart grid information systems.

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

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

Requirement

1. Systems that provide name/address resolution services are configured to provide additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries; and
2. Systems that provide name/address resolution to smart grid information systems, when operating as part of a distributed, hierarchical namespace, are configured 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

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. Failure to a known state may include digital, analog, or other modes of operation.

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

Refer to SG.SC-12 for additional information. Additional guidance on protecting the confidentiality of customer information is provided in NISTIR 7628, Volume 2, Chapter 5.

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 smart grid information system is implemented with diverse technologies.

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 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

Requirement

The smart grid information system is partitioned into components 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

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 Technical Requirements

Requirement

1. The smart grid information system—
   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
   c. 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 Technical Requirements

Requirement

The smart grid information system monitors events 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 organization management authority is notified when anomalies are discovered on smart grid information systems.

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,

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

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

3.26 TESTING AND CERTIFICATION OF SMART GRID CYBERSECURITY

The testing and certification of the smart grid cybersecurity requirements provide assurance that systems and system components are conformant to the requirements selected by the organization. The use of consistent, standardized cybersecurity evaluation criteria and methodologies contributes to the repeatability and objectivity of test results, which provide insight into the extent to which the requirements are implemented correctly, operating as intended, and producing the desired security posture for the smart grid information system and system components. Understanding the overall effectiveness of the security requirements implemented in the smart grid information system and its operational environment is essential in determining the risk to the organization's operations.

The Guide for Assessing the High-Level Security Requirements in NISTIR 7628 [33] (*The Guide*) provides a set of guidelines for building effective security assessment plans and a baseline set of procedures for assessing the effectiveness of security requirements employed in smart grid information systems. *The Guide* is written to provide a foundation to facilitate a security assessment based on the high-level security requirements identified earlier in this chapter, implemented within an effective risk management program. It includes descriptions of the basic

[33] *Guide for Assessing the High-Level Security Requirements in NISTIR 7628*, Version 1.0, August 24, 2012. https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/NISTIR_7628_Assessment_Guide-v1p0-24Aug2012.pdf

concepts needed when assessing the high-level security requirements in smart grid information systems, the Security Assessment process (including specific activities carried out in each phase of the assessment), the assessment method definitions, the Assessment Procedures Catalog and a Sample Security Assessment Report outline. Additionally, the Assessment Procedures Catalog has been placed in a companion spreadsheet tool[34] for assessors that can be used to record the findings of an assessment and used as the basis for the development of a final assessment report.

The objective of security assessments is to verify that the implementers and operators of smart grid information systems are meeting their stated objectives. The security assessment process involves participation and buy-in from both the assessor and organizational stakeholders. Key organizational participants in the process include senior management, smart grid information system and industrial control system owners, and the Chief Information Security Officer. The result of the security assessment provides realistic information to senior management about the risk posture and residual risks of the smart grid information system, which will form the basis for any decision to approve or authorize the system for operation.

However, cybersecurity testing does not operate in a vacuum; these efforts should be performed in coordination with interoperability testing to ensure that changes to one do not adversely impact the operation of the other. For instance, as a functionality is developed to enable interoperability, new potential vulnerabilities can be introduced. By ensuring that cybersecurity testing is coordinated with interoperability testing, design, implementation and operational flaws that could allow the violation of cybersecurity requirements, and loopholes that can cause loss of information, availability, or allow unauthorized access can be identified and mitigated.

The Smart Grid Interoperability Panel (SGIP) Smart Grid Testing and Certification Committee (SGTCC) developed and issued an *Interoperability Process Reference Manual* (IPRM) Version 2.0[35] in January 2012 that details its recommendations on processes and best practices that enhance the introduction of interoperable products in the marketplace. These recommendations build upon international standards-based processes (ISO/IEC 17025 and ISO/IEC Guide 65) for interoperability testing and certification for testing laboratories and certification body management systems. Additionally, the IPRM identifies technical requirements and best practices necessary to help assure testing programs' technical depth and sufficiency for interoperability and cybersecurity. The IPRM Version 2.0 includes sections that discuss: International Guidelines for Testing and Certification, ITCA Implementation of the IPRM, Interoperability and Conformance Test Construction, Cybersecurity Testing, and Interoperability Certification Body and Testing Laboratory Requirements.

The SGTCC asserts that implementation of the IPRM by Interoperability Testing and Certification Authorities (ITCAs) will increase the quality of standards-based, secure and interoperable products in the smart grid marketplace. Implementation of the IPRM will lead to reduced deployment costs of smart grid systems and devices, and enhanced product quality with respect to interoperability and conformance. This will ultimately provide increased end-user customer satisfaction and confidence to the buyer through meaningful certification programs. For instance, as electric utilities turn to Advanced Metering Infrastructures (AMIs) to promote the development and deployment of the smart grid, one aspect that can benefit from

[34] The Companion Spreadsheet to the *Guide for Assessing the High-Level Security Requirements in NISTIR 7628* is available at: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/2012-004_1_Companion_Spreadsheet.docx

[35] *IPRM Version 2.0*, January 2012. https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SmartGridTestingAndCertificationCommittee/IPRM_final_-_011612.pdf

standardization is the upgradeability of Smart Meters. The National Electrical Manufacturers Association (NEMA) standard SG-AMI 1-2009, *Requirements for Smart Meter Upgradeability*, describes functional and security requirements for the secure upgrade—both local and remote—of smart meters. Draft NISTIR 7823, *Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework*, describes conformance test requirements that may be used voluntarily by testers and/or test laboratories to determine whether smart meters and upgrade management systems conform to the requirements of NEMA SG-AMI 1-2009.

CHAPTER 4
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 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. It is expected 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 in software. 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 communication 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 the design of 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 [§4.4-1] 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 a 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, leaving customers to figure out how to provision all their devices with secret keys or

digital 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. Key provisioning should be 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. Alternatively, 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 where the private key never leaves the HSM, higher levels of security with lower associated operational costs are provided. 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 PKI 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 (CP) Object Identifiers (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 or outsource individual PKIs. 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. Distinguished names (DNs) offer 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 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, 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, for example. [4.4-24] When multiple organizations are endeavoring to provide 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. 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. The mesh model is likely to be too expensive. 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. For large inter-domain systems, a federated approach is the most reasonable solution for large inter-domain systems.

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. Utility 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 the organization is the rightful owner of the domain name listed in the 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 CP 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 RP. 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 CP Extension. The CP Extension contains an Object ID (OID) 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, reducing 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

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.[36] 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:

- ***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

[36] This certificate lifetime recommendation for smart grid applications is not intended to conflict with the 20 year certificate lifetime upper bound recommended by the X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework. Based on the operational requirements of smart grid applications, a lower upper bound for the certificate lifetime is recommended.

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.
- ***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) and 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. Additionally, in accordance with RFC 2560, no revocation check is required for manufacturers' device management certificates.

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 [§4.4-22], 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) [§4.4-4]
- ***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 Revision 2 (using the curves with 256- and 384-bit prime moduli) [§4.4-9]
- ***Digital Signature***. Elliptic Curve Digital Signature Algorithm (ECDSA) – FIPS PUB 186-3 (using the curves with 256 and 384-bit prime moduli) [§4.4-3]
- ***Hashing***. Secure Hash Algorithm (SHA) –- FIPS PUB 180-4 (using SHA-256 and SHA-384) [§4.4-2]

Intellectual Property issues have been cited pertaining to the adoption of ECC. To mitigate these issues NSA has stated:

> 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. [§4.4-22][37]

A number of questions arise when considering this license for smart grid use:

1. How can vendors interesting in developing 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 RFC 6090 titled "Fundamental Elliptic Curve Cryptography Algorithms." [4.4-23]

Intellectual property rights (IPR) statements and frequently asked questions (FAQs) covering pricing have been made concerning some commercial use of patented ECC technology.[38] 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.

---

[37] *See*, http://www.nsa.gov/ia/contacts/index.shtml for more information.

[38] *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

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 (Revision 3)* [4.4-11], 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 makes use of cryptography, and they are a starting point for smart grid key management.[39]

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 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 became public. For this reason, FIPS-approved and NIST-recommended cryptographic techniques are strongly recommended, 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

[39] *See* Volume 3, Chapter 8 R&D for a discussion of some of the considerations.

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 should 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 needs 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[40] has published many 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 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 a 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.

[40] *See*, http://csrc.nist.gov.

- 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 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)*. [§4.4-14]

NIST has also published NIST SP 800-22 Revision 1a, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* [§4.4-7], 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.

For example, if a system is set up to allow external emergency workers to have access to the devices without authenticating to the devices, the devices should have different access modes which may be selected by only authorized personnel. An exclusive defined set of operations is allowed in each access mode. Prior to granting access to external emergency works, identity verification should be completed.

4.2.1.6 Availability

Availability for some 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: Part 1(Revision 3)* [§4.4-11] 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 case, if an employee's status changes and it becomes necessary to revoke his/her certificate, this certificate would only need to be maintained on the CRL until the certificate expiration date; allowing the CRL to 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 because the likelihood of needing to revoke a certificate is low. Therefore, the CRLs would not be expected to be very large. In case a smart grid RP receives an expired certificate from an entity (a person or device), the RP can accept the certificate and authenticate the entity, or the RP can reject the certificate, potentially resulting in a major system malfunction.

Since smart grid devices will be deployed with the intent to keep them operational for 10 to 15 years, replacing these devices will not occur very often. However, 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 it can be guaranteed that their keys are 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 year to retry to obtain a new certificate. 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.

Due to 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 (updated by RFC 6818). 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 [4.4-18][41], 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,

[41] OCSP is specified in RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* (standards track). For more information on OCSP, see section 4.2.2.1.5 where OCSP is discussed in detail.

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 natural disaster, that resources would be sent across the country from sources that were never anticipated. There are 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 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.
- 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 and 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 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 to 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 to 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 OCSP, 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; and 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 returns 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 CAs 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 kB to 12 kB of RAM and 64 kB to 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 [§4.4-17] 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) [§4.4-19] supports multiple authentication methods called EAP methods, and its key management framework [§4.4-20] 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 [§4.4-21]. EAP therefore can be a basis of SSO for smart meters. RFC 5295 [§4.4-21] 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 the data. This poses important challenges in the management of these keys. The primary considerations that encompass symmetric key management include 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 one of the greatest challenges 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[42]—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 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.

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.

[42] 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 where connectivity to the encryption platform has been lost and field personnel need to physically transport the keys to the encryption platform.

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 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[43] prior to usage in order to ensure continuous communications. It should be noted that key roll over and the roll over 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 (confidentiality, integrity, and availability) requirements. The source material that will be used to build these cryptographic requirements is in [§2.2] and [§3.4]. 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.

[43] A crypto group is a group of end devices that share a common symmetric key thereby creating a cryptographic group.

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 were made to ensure recommendations are 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 [4.4-11] should be used, as these requirements are not governed by content 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 baseline 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 these two Special Publications (SPs) 800-57 [§4.4-11] and SP 800-131A, *Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes* [§4.4-16]. Validation and conformance testing of cryptographic modules implementing NIST-approved algorithms is specified in FIPS 140-2 [§4.4-1].

It is important to note the following points:

- SP 800-131A was published in January 2011 and timelines for several algorithms transitions had been changed since its draft version.
- 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 800-131A.
- Cryptographic information described in this NISTIR is mainly derived from general requirements specified in those two SPs.

4.3.2.1.2 Background

All of the cryptographic algorithms that are required for use in the smart grid should 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/SGCC is chartered to coordinate cybersecurity standards for the smart grid. Since one of the primary goals is interoperability, the CSWG/SGCC needs to ensure that any standards under consideration be usable by all stakeholders of the smart grid.

In the area of cryptography, federal law[44] requires that U.S. federal government entities must use NIST-approved or allowed algorithms. From FIPS-140-2:

> 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 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. [§4.4-1]

Given that many participants in the smart grid (including AMI) are U.S. federal agencies, interoperability requires that CSWG/SGCC-listed standards be usable by them. Examples are the Tennessee Valley Authority, Bonneville Power Administration, and military bases around the world.[45]

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.

NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, includes the following tables that describe the transition schedules for:

- Table 1: Encryption Algorithms
- Table 2: Digital Signatures Security Strength
- Table 3: Random Number Generation
- Table 4: SP 800-56A Key Agreement (Diffie-Helman and MQV)
- Table 5: EC Parameter Sets
- Table 6: RSA-based Key Agreement and Key Transport Key Length Transitions
- Table 7: Symmetric Key Wrapping Key Length Transitions
- Table 8: Key Length Transitions for a Key Derivation Function (KDF)
- Table 9: Hash Function Transitions
- Table 10: Message Authentication Code Transitions

[44] The Federal Information Security Management Act of 2002 (Pub. L. 107-347 (Title III)); the Information Technology Management Reform Act of 1996

[45] 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.

NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revision 3)*, includes the following tables that describe:

- Table 2: Comparable (Security) Strengths
- Table 3: Has Function That Can Be Used to Provide the Targeted Security Strengths

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 protections 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 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 in line with established and known good methods, such as those listed in FIPS-140-2.
- **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 4-1 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 appropriate 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 in security of the entire system.	NIST SP 800-57, Section 5.2
		X	X	All root key material should 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	Should always be locally autonomous. That is no authentication process should 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 should 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 should 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) should be protected throughout the distribution process.
				• During manual distribution, secret or private keys should either be encrypted or be distributed using appropriate physical security procedures.
				  ○ The distribution should be from an authorized source,
				  ○ 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
				○ The keys are protected in accordance with Section 6 [800-57], and ○ 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. Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 25, 2001 (including change notices through December 3, 2002), 69 pp. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [accessed 8/11/2014].
2. FIPS 180-4, *Secure Hash Standard (SHS)*, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2012, 37 pp. http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf [accessed 8/11/2014].
3. FIPS 186-4, *Digital Signature Standard (DSS)*, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 130 pp. http://dx.doi.org/10.6028/NIST.FIPS.186-4 (redirects to: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).
4. FIPS 197, *Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, Gaithersburg, Maryland, November 26, 2001, 51 pp. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [accessed 8/11/2014].
5. FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2008, 13 pp. http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf [accessed 8/11/2014].
6. E. Barker, W. Barker, and A. Lee, *Guideline for Implementing Cryptography in the Federal Government*, NIST Special Publication (SP) 800-21 Second Edition, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2005, 97 pp. http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf [accessed 8/11/2014].
7. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, and L. Bassham, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST SP 800-22 Revision 1a, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2010, 131 pp. http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf [accessed 8/11/2014].
8. D.R. Kuhn, V.C. Hu, W.T. Polk, and S.-J. Chang, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, NIST SP 800-32, National Institute of Standards and Technology, Gaithersburg, Maryland, February 26, 2001. http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf [accessed 8/11/2014].
9. E. Barker, L. Chen, A. Roginsky, and M. Smid, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, NIST SP 800-56A Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, 138 pp. http://dx.doi.org/10.6028/NIST.SP.800-56Ar2 (redirects to: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf).
10. E. Barker, L. Chen, A. Regenscheid, and M. Smid, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, NIST SP 800-56B,

National Institute of Standards and Technology, Gaithersburg, Maryland, August 2009, 114 pp. http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf [accessed 8/11/2014].

11. NIST SP 800-57, *Recommendation for Key Management* (Parts 1, 2 and 3):

    E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, *Recommendation for Key Management—Part 1: General (Revision 3)*, NIST SP 800-57 Part 1 Revision 3, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2012, 147 pp. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf [accessed 8/11/2014].

    E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, *Recommendation for Key Management—Part 2: Practices for Key Management Organization*, NIST SP 800-57 Part 2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2005, 79 pp. http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf [accessed 8/11/2014].

    E. Barker, W. Burr, A. Jones, T. Polk, S. Rose, Q. Dang, and M. Smid, *Recommendation for Key Management—Part 3: Application-Specific Key Management Guidance*, NIST SP 800-57 Part 3, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2009, 103 pp. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf [accessed 8/11/2014].

12. R. Chandramouli and Scott Rose, *Secure Domain Name System (DNS) Deployment Guide*, NIST SP 800-81-2, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2013, 130 pp. http://dx.doi.org/10.6028/NIST.SP.800-81-2 (redirects to: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf).

13. E. Barker, *Recommendation for Obtaining Assurances for Digital Signature Applications*, NIST SP 800-89, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2006, 38 pp. http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf [accessed 8/11/2014].

14. NIST SP 800-90 (A, B and C):

    E. Barker and J. Kelsey, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, NIST SP 800-90A, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2012, 136 pp. http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf [accessed 8/11/2014].

    E. Barker and J. Kelsey, *Recommendation for the Entropy Sources Used for Random Bit Generation*, DRAFT NIST SP 800-90B, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2012, 78 pp. http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf [accessed 8/11/2014].

    E. Barker and J. Kelsey, *Recommendation for Random Bit Generator (RBG) Constructions*, DRAFT NIST SP 800-90C, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2012, 50 pp. http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90c.pdf [accessed 8/11/2014].

15. E. Barker, *Recommendation for Digital Signature Timeliness*, NIST SP 800-102, National Institute of Standards and Technology, Gaithersburg, Maryland, Septebmer 2009, 30 pp. http://csrc.nist.gov/publications/nistpubs/800-102/sp800-102.pdf [accessed 8/11/2014].

16. E. Barker and A. Roginsky, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, NIST SP 800-131A, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2011, 27 pp. http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf [accessed 8/11/2014].

17. American National Standard Institute (ANSI), *Protocol Specification for Interfacing to Data Communication Networks*, ANSI C12.22-2008, National Electrical Manufacturers Association (NEMA), Rosslyn, Virginia, 2008.

18. S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, IETF Network Working Group RFC 6960, June 2013. http://www.ietf.org/rfc/rfc6960.txt [accessed 8/11/2014].

19. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, *Extensible Authentication Protocol (EAP)*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 3748, June 2004. http://www.ietf.org/rfc/rfc3748.txt [accessed 8/11/2014].

20. B. Aboba, D. Simon, and P. Eronen, *Extensible Authentication Protocol (EAP) Key Management Framework*, IETF Network Working Group RFC 5247, August 2008. http://www.ietf.org/rfc/rfc5247.txt [accessed 8/11/2014].

21. J. Salowey, L. Dondeti, V. Narayanan, and M. Nakhjiri, *Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)*, IETF Network Working Group RFC 5295, August 2008. http://www.ietf.org/rfc/rfc5295.txt [accessed 8/11/2014].

22. Department of Defense, National Security Agency, *Suite B Cryptography* [Web page], http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml [accessed 8/11/2014].

23. D. McGrew, K. Igoe, and M. Salter, "*Fundamental Elliptic Curve Cryptography Algorithms*," IETF Network Working Group RFC 6090, February 2011.

24. R. Housley, and T. Polk, *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*, Wiley, NY, NY, March 2001, 352 pp.

APPENDIX A
CROSSWALK OF CYBERSECURITY DOCUMENTS

This Appendix includes a crosswalk of cybersecurity requirements of NISTIR 7628 with key source documents, NIST SP 800-53 Rev. 4 and the DHS Catalog[46], and other standards[47] relevant to the smart grid. The crosswalk is not an exhaustive mapping of all cybersecurity requirements and best practices applicable to the smart grid.

Table A-1 Crosswalk of Cybersecurity Requirements and Documents

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
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 003-3 (R1, R5, R5.2, R5.3) CIP 005-3a (R1, R1.1, R1.6) CIP 006-3c (R2)
SG.AC-2	Remote Access Policy and Procedures	AC-17	Remote Access	2.15.23	Remote Access Policy and Procedures	CIP 005-3a (R1, R1.1, R1.2, R1.6, R2, R2.3, R2.4) CIP 007-3a (R5)
SG.AC-3	Account Management	AC-2	Account Management	2.15.3	Account Management	CIP 003-3 (R5, R5.1, R5.2, R5.3) CIP 004-3a (R4, R4.1, R4.2) CIP 005-3a (R2.5.1, R2.5.3) CIP 007-3a (R5, R5.1, R5.1.3, R5.2, R5.2.3)
SG.AC-4	Access Enforcement	AC-3	Access Enforcement	2.15.7	Access Enforcement	CIP 004-3a (R4)

[46] Department of Homeland Security, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers*, version 7, April 2011. https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf [accessed 8/11/2014].

[47] North American Electric Reliability Corporation (NERC), *CIP [Critical Infrastructure Protection] Standards* [Web page], http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx [accessed 8/11/2014].

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
						CIP 005-3a (R1.6, R2, R2.1-R2.4) CIP 007-3a (R5)
SG.AC-5	Information Flow Enforcement	AC-4	Information Flow Enforcement	2.15.15	Information Flow Enforcement	None
SG.AC-6	Separation of Duties	AC-5	Separation of Duties	2.15.8	Separation of Duties	CIP 005-3a (R2, R2.1) CIP 007-3a (R5.1, R5.2)
SG.AC-7	Least Privilege	AC-6	Least Privilege	2.15.9	Least Privilege	CIP 007-3a (R5.1, R5.2)
SG.AC-8	Unsuccessful Login Attempts	AC-7	Unsuccessful Login Attempts	2.15.20	Unsuccessful Logon Notification	CIP 007-3a (R5)
SG.AC-9	Smart Grid Information System Use Notification	AC-8	System Use Notification	2.15.17	System Use Notification	CIP 005-3a (R2.6)
SG.AC-10	Previous Logon Notification	AC-9	Previous Logon (Access) Notification	2.15.19	Previous Logon Notification	None
SG.AC-11	Concurrent Session Control	AC-10	Concurrent Session Control	2.15.18	Concurrent Session Control	None
SG.AC-12	Session Lock	AC-11	Session Lock	2.15.21	Session Lock	None
SG.AC-13	Remote Session Termination			2.15.22	Remote Session Termination	CIP 007-3a (R6)
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	None
SG.AC-15	Remote Access	AC-17	Remote Access	2.15.24	Remote Access	CIP 005-3a (R2, R2.1-R2.5, R3, R3.1, R3.2) CIP 007-3a (R2.1, R5)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.AC-16	Wireless Access Restrictions			2.15.26	Wireless Access Restrictions	CIP 005-3a (R1.1, R2, R2.4, R3, R3.2)
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 005-3a (R2, R2.1, R2.2, R2.4, R3, R3.2)
SG.AC-18	Use of External Information Control Systems	SC-7	Boundary Protection	2.15.29	Use of External Information Control Systems	CIP 005-3a (R2.4)
SG.AC-19	Control System Access Restrictions			2.15.28	External Access Protections	CIP 005-3a (R1.6) CIP 007-3a (R5)
SG.AC-20	Publicly Accessible Content	AC-22	Publicly Accessible Content			None
SG.AC-21	Passwords			2.15.16	Passwords	CIP 007-3a (R5.3, R5.3.3)
Awareness and Training (SG.AT)						
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 003-3 (R1, R2, R3) CIP 004-3a (R1, R2.1, R2.3)
SG.AT-2	Security Awareness	AT-2	Security Awareness	2.11.2	Security Awareness	CIP 004-3a (R1)
SG.AT-3	Security Training	AT-3	Security Training	2.11.3	Security Training	CIP 004-3a (R2, R2.1)
SG.AT-4	Security Awareness and Training Records	AT-4	Security Training Records	2.11.4	Security Training Records	CIP 004-3a (R2.3)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.AT-5	Contact with Security Groups and Associations	PM-15	Contacts with Security Groups and Associations	2.11.5	Contact with Security Groups and Associations	None
SG.AT-6	Security Responsibility Training	PM-14	Testing, Training, and Monitoring	2.11.6	Security Responsibility Training	CIP 004-3a (R2, R2.1, R2.2)
SG.AT-7	Planning Process Training	PM-14	Testing, Training, and Monitoring	2.7.5	Planning Process Training	CIP 004-3a (R2, R2.2)
Audit and Accountability (SG.AU)						
SG.AU-1	Audit and Accountability Policy and Procedures	AU-1	Audit and Accountability Policy and Procedures	2.16.1	Audit and Accountability Process and Procedures	CIP 003-3a (R1, R2, R3, R5.3) CIP 007-3a (R5, R5.1.2, R5.2.3, R6.3-R6.5, R7.3, R9)
SG.AU-2	Auditable Events	AU-2	Audit Events	2.16.2	Auditable Events	CIP 005-3a (R3.2) CIP 006-3c (R7) CIP 007-3a (R5.1.2, R5.2.3, R6, R6.1, R6.3, R6.5)
SG.AU-3	Content of Audit Records	AU-3	Content of Audit Records	2.16.3	Content of Audit Records	CIP 007-3a (R5.1.2, R6, R6.3)
SG.AU-4	Audit Storage Capacity	AU-4	Audit Storage Capacity	2.16.4	Audit Storage	CIP 007-3a (R6.1)
SG.AU-5	Response to Audit Processing Failures	AU-5	Response to Audit Processing Failures	2.16.5	Response to Audit Processing Failures	CIP 007-3a (R6.1)
SG.AU-6	Audit Monitoring, Analysis, and Reporting	AU-6	Audit Monitoring, Analysis, and Reporting	2.16.6	Audit Monitoring, Process, and Reporting	CIP 004-3a (R3, R4.2, R4.2) CIP 005-3a (R3.2) CIP 007-3a (R5.1.2, R6.5)
SG.AU-7	Audit Analysis Tools and Report Generation	AU-7	Audit Reduction and Report Generation	2.16.7	Audit Reduction and Report Generation	CIP 007-3a (R5.1.2, R6.5)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.AU-8	Time Stamps	AU-8	Time Stamps	2.16.8	Time Stamps	CIP 007-3a (R5.1.2, R6.3)
SG.AU-9	Protection of Audit Information	AU-9	Protection of Audit Information	2.16.9	Protection of Audit Information	CIP 003-3 (R4, R4.1, R5)
SG.AU-10	Audit Record Retention	AU-11	Audit Record Retention	2.16.10	Audit Record Retention	CIP 005-3a (R5.3) CIP 007-3a (R5.1.2, R6.4) CIP 008-3 (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	CIP 002-3 (R1) CIP 003-3 (R1.3, R4.3, R5.2) CIP 005-3a (R5.1)
SG.AU-12	Auditor Qualification			2.16.12	Auditor Qualification	None
SG.AU-13	Audit Tools	AU-7	Audit Reduction and Report Generation	2.16.13	Audit Tools	CIP 007-3a (R6)
SG.AU-14	Security Policy Compliance	CA-1	Security Assessment and Authorization Policies and Procedures	2.16.14	Security Policy Compliance	CIP 003-3 (R1.3, R4.3, R5.2) CIP 005-3a (R5.1) CIP 008-3 (R1.4, R1.5, R1.6) CIP 009-3 (R2, R3, R5)
SG.AU-15	Audit Generation	AU-12	Audit Generation	2.16.15	Audit Generation	CIP 007-3a (R6)
SG.AU-16	Non-Repudiation	AU-10	Non-Repudiation	2.16.16	Non-Repudiation	CIP 003-3 (R6)
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 Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
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	CIP 003-3 (R3.3, R4.3) CIP 005-3a (R4.5) CIP 006-3c (R1.7, R8) CIP 007-3a (R1, R1.1, R2, R2.3, R3.2)
				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	CIP 003-3 (R3, R4.3) CIP 005-3a (R4) CIP 007-3a (R1, R1.1)
SG.CA-3	Continuous Improvement			2.17.2	Continuous Improvement	CIP 007-3a (R3, R3.2, R4, R4.2)
				2.17.4	Best Practices	
SG.CA-4	Smart Grid Information System Connections	CA-3	System Interconnections	2.18.5	Control System Connections	CIP 005-3a (R1.3, R1.6, R2, R2.5, R3, R3.1, R3.2, R4.3, R5.1) CIP 006-3c (R5) CIP 007-3a (R2)
		CA-9	Internal System Connections			
SG.CA-5	Security Authorization to Operate	CA-6	Security Authorization	2.17.5	Security Accreditation	CIP 003-3 (R2, R2.2, R3.3)
		PM-10	Security Authorization Process			
SG.CA-6	Continuous Monitoring	CA-7	Continuous Monitoring	2.18.7	Continuous Monitoring	CIP 003-3 (R3.3, R4.3) CIP 005-3a (R4.5) CIP 006-3c (R1.7, R8)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
						CIP 007-3a (R1, R1.1, R2, R2.3, R3.2)
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 003-3 (R1, R2, R3, R3.3, R4, R4.1, R4.2, R4.3, R6) CIP 005-3a (R2.2, R5, R5.1, R5.2) CIP 007-3a (R9)
SG.CM-2	Baseline Configuration	CM-2	Baseline Configuration	2.6.2	Baseline Configuration	CIP 003-3 (R4) CIP 005-3a (R5.1) CIP 006-3c (R1.2) CIP 007-3a (R2, R9)
SG.CM-3	Configuration Change Control	CM-3	Configuration Change Control	2.6.3	Configuration Change Control	CIP 003-3 (R6) CIP 005-3a (R5.1, R5.2) CIP 007-3a (R1, R1.1, R1.2, R1.3, R3, R3.1, R3.2, R4.2, R9)
		SA-10	Developer Configuration Management			
SG.CM-4	Monitoring Configuration Changes	CM-4	Security Impact Analysis	2.6.4	Monitoring Configuration Changes	CIP 003-3 (R6) CIP 007-3a (R1, R1.1, R1.2, R1.3, R3, R3.1)
		SA-10	Developer Configuration Management			
SG.CM-5	Access Restrictions for Configuration Change	CM-5	Access Restrictions for Change	2.6.5	Access Restrictions for Configuration Change	CIP 003-3 (R6) CIP 007-3a (R1, R5, R5.1, R5.1.2, R5.1.3, R5.2, R5.2.3)
SG.CM-6	Configuration Settings	CM-6	Configuration Settings	2.6.6	Configuration Settings	CIP 003-3 (R2.4, R3, R3.1, R3.2, R3.3, R6)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
						CIP 005-3a (R2.2) CIP 007-3a (R2.1 – R2.3, R3.2, R4.1, R9)
SG.SC	Configuration for Least Functionality	CM-7	Least Functionality	2.6.7	Configuration for Least Functionality	CIP 005-3a (R2.2, R4.2) CIP 007-3a (R2, R2.1, R2.2, R8.2)
SG.CM-8	Component Inventory	CM-8	Information System Component Inventory	2.6.8	Configuration Assets	CIP 003-3 (R6) CIP 005-3a (R1, R1.2 – R1.4, R1.6, R2, R5.1, R5.2) CIP 006-3c (R1.1) CIP 007-3a (R3.2, R7.3, R9)
		PE-20	Asset Monitoring and Tracking			
SG.CM-9	Addition, Removal, and Disposal of Equipment	MP-6	Media Sanitization	2.6.9	Addition, Removal, and Disposition of Equipment	CIP 003-3 (R6) CIP 007-3a (R7, R7.1, R7.2, R7.3)
SG.CM-10	Factory Default Settings Management			2.6.10	Factory Default Authentication Management	CIP 005-3a (R4.4) CIP 007-3a (R5.2.1, R8.3)
SG.CM-11	Configuration Management Plan	CM-9	Configuration Management Plan			CIP 003-3 (R6)
Continuity of Operations (SG.CP)						
SG.CP-1	Continuity of Operations Policy and Procedures	CP-1	Contingency Planning Policy and Procedures			CIP 003-3 (R1, R2, R3) CIP 009-3 (R1, R4)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.CP-2	Continuity of Operations Plan	CP-1	Contingency Planning Policy and Procedures	2.12.2	Continuity of Operations Plan	CIP 008-3 (R1) CIP 009-3 (R1, R1.2, R4)
SG.CP-3	Continuity of Operations Roles and Responsibilities	CP-2	Contingency Plan	2.12.3	Continuity of Operations Roles and Responsibilities	CIP 009-3 (R1.1, R1.2)
SG.CP-4	Continuity of Operations Training					CIP 004-3a (R2.2.4)
SG.CP-5	Continuity of Operations Plan Testing	CP-4	Contingency Plan Testing and Exercises	2.12.5	Continuity of Operations Plan Testing	CIP 007-3a (R1.1, R1.2, R1.3, R9) CIP 008-3 (R1.6) CIP 009-3 (R2, R5)
SG.CP-6	Continuity of Operations Plan Update	CP-2	Contingency Plan	2.12.6	Continuity of Operations Plan Update	CIP 009-3 (R1, R3)
SG.CP-7	Alternate Storage Sites	CP-6	Alternate Storage Sites	2.12.13	Alternative Storage Sites	CIP 009-3 (R4)
SG.CP-8	Alternate Telecommunication Services	CP-8	Telecommunications Services	2.12.14	Alternate Command/Control Methods	CIP 009-3 (R4)
SG.CP-9	Alternate Control Center	CP-7	Alternate Processing Site	2.12.15	Alternate Control Center	CIP 009-3 (R4)
		CP-8	Telecommunications Services			
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 003-3 (R4.1) CIP 005-3a (R4.4) CIP 007-3a (R8.3) CIP 009-3 (R4)
SG.CP-11	Fail-Safe Response	CP-12	Safe Mode	2.12.18	Fail-Safe Response	CIP 009-3 (R4)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
		SI-17	Fail-Safe Procedures			
Identification and Authentication (SG.IA)						
SG.IA-1	Identification and Authentication Policy and Procedures	IA-1	Identification and Authentication Policy and Procedures	2.15.2	Identification and Authentication Procedures and Policy	CIP 003-3 (R1, R2, R3) CIP 005-3a (R2.4, R2.5.1-R2.5.3) CIP 007-3a (R5, R9)
SG.IA-2	Identifier Management	IA-4	Identifier Management	2.15.4	Identifier Management	CIP 007-3a (R5.1.1)
SG.IA-3	Authenticator Management	IA-5	Authenticator Management	2.15.5	Authenticator Management	CIP 005-3a (R4.4) CIP 007-3a (R5, R5.1, R5.1.1, R5.3)
SG.IA-4	User Identification and Authentication	IA-2	User Identification and Authentication	2.15.10	User Identification and Authentication	CIP 005-3a (R2.4) CIP 007-3a (R5)
SG.IA-5	Device Identification and Authentication	IA-3	Device Identification and Authentication	2.15.12	Device Authentication and Identification	CIP 005-3a (R2)
SG.IA-6	Authenticator Feedback	IA-6	Authenticator Feedback	2.15.13	Authenticator Feedback	CIP 007-3a (R5)
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	CIP 003-3 (R1,R2, R3, R4.1, R4.3, R5, R5.2, R5.3) CIP 005-3a (R1.6, R4.1, R5, R5.3) CIP 007-3a (R7, R9) CIP 008-3 (R2)
SG.ID-2	Information and Document Retention	SI-12	Information Output Handling and Retention	2.9.2	Information and Document Retention	CIP 005-3a (R1.6, R2.6, R5, R5.1 – R5.3)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
						CIP 006-3c (R7) CIP 007-3a (R6.3 – R6.5, R7.3)
SG.ID-3	Information Handling	MP-1	Media Protection Policy and Procedures	2.9.3	Information Handling	CIP 003-3 (R4.1) CIP 007-3a (R7, R7.3)
SG.ID-4	Information Exchange			2.9.5	Information Exchange	None
SG.ID-5	Automated Labeling			2.9.11	Automated Labeling	None
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	CIP 003-3 (R1, R2, R3) CIP 008-3 (R1, R1.1, R2)
SG.IR-2	Incident Response Roles and Responsibilities	IR-1	Incident Response Policy and Procedures	2.7.4	Roles and Responsibilities	CIP 003-3 (R2, R2.3) CIP 008-3 (R1.2, R1.3) CIP 009-3 (R1.2)
SG.IR-3	Incident Response Training	IR-2	Incident Response Training	2.12.4	Incident Response Training	CIP 004-3a (R2.2.4, R2.3)
SG.IR-4	Incident Response Testing and Exercises	IR-3	Incident Response Testing			CIP 007-3a (R1.1, R1.2, R1.3) CIP 008-3 (R1.6) CIP 009-3 (R2)
SG.IR-5	Incident Handling	IR-4	Incident Handling	2.12.7	Incident Handling	CIP 009-3 (R1.1, R3)
SG.IR-6	Incident Monitoring	IR-5	Incident Monitoring	2.12.8	Incident Monitoring	CIP 005-3a (R5.3) CIP 006-3c (R7) CIP 008-3 (R1.2, R2)
SG.IR-7	Incident Reporting	IR-6	Incident Reporting	2.12.9	Incident Reporting	CIP 008-3 (R1.1, R1.3)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.IR-8	Incident Response Investigation and Analysis	PE-6	Monitoring Physical Access	2.12.11	Incident Response Investigation and Analysis	CIP 008-3 (R1.4)
SG.IR-9	Corrective Action	SI-11	Error Handling	2.12.12	Corrective Action	CIP 008-3 (R1.4) CIP 009-3 (R3)
SG.IR-10	Smart Grid Information System Backup	CP-9	Information System Backup	2.12.16	Control System Backup	CIP 009-3 (R4)
SG.IR-11	Coordination of Emergency Response	IR-10	Integrated Information Security Analysis Team	2.2.4	Coordination of Threat Mitigation	CIP 004-3a (R2.1, R2.2.4) CIP 008-3 (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	CIP 003-3 (R1, R2, R3) CIP 006-3c (R8) CIP 007-3a (R9)
SG.MA-2	Legacy Smart Grid Information System Upgrades			2.10.2	Legacy System Upgrades	CIP 003-3 (R6) CIP 007-3a (R1)
SG.MA-3	Smart Grid Information System Maintenance	PL-6	Security-Related Activity Planning	2.10.5	Unplanned System Maintenance	CIP 007-3a (R7, R7.2) CIP 009-3 (R4)
		MA-2	Controlled Maintenance	2.10.6	Periodic System Maintenance	
SG.MA-4	Maintenance Tools	MA-3	Maintenance Tools	2.10.7	Maintenance Tools	CIP 007-3a (R7)
SG.MA-5	Maintenance Personnel	MA-5	Maintenance Personnel	2.10.8	Maintenance Personnel	CIP 007-3a (R5, R5.2)
SG.MA-6	Remote Maintenance	MA-4	Nonlocal Maintenance	2.10.9	Remote Maintenance	CIP 003-4 (R5)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
						CIP 005-3a (R2, R2.3, R2.5.4, R3.1, R3.2)
SG.MA-7	Timely Maintenance	MA-6	Timely Maintenance	2.10.10	Timely Maintenance	CIP 009-3 (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	CIP 003-3 (R1, R2, R3, R4, R4.1, R4.3) CIP 004-3a (R2.2.3) CIP 007-3a (R9)
SG.MP-2	Media Sensitivity Level	RA-2	Security Categorization	2.13.3	Media Classification	CIP 003-3 (R4, R4.2)
				2.9.4	Information Classification	
SG.MP-3	Media Marketing	MP-3	Media Marketing	2.13.4	Media Labeling	CIP 003-3 (R4, R4.1)
				2.9.10	Automated Marking	
SG.MP-4	Media Storage	MP-4	Media Storage	2.13.5	Media Storage	CIP 006-3c (R1.1)
SG.MP-5	Media Transport	MP-5	Media Transport	2.13.6	Media Transport	CIP 003-3 (R5.1) CIP 007-3a (R7)
SG.MP-6	Media Sanitization and Disposal	MP-6	Media Sanitization	2.13.7	Media Sanitization and Storage	CIP 007-3a (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 003-3 (R1, R2, R3) CIP 005-3a (R1.6) CIP 006-3c (R1, R2, R7, R8)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
						CIP 007-3a (R9)
SG.PE-2	Physical Access Authorizations	PE-2	Physical Access Authorizations	2.4.2	Physical Access Authorizations	CIP 003-3 (R5.1) CIP 004-3a (R3, R4, R4.1) CIP 006-3c (R1.5)
SG.PE-3	Physical Access	PE-3	Physical Access Control	2.4.3	Physical Access Control	CIP 004-3a (R4) CIP 006-3c (R2, R4, R3) CIP 007-3a (R5, R5.2.3)
		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 006-3c (R1.3, R4, R5, R6) CIP 008-3 (R1)
SG.PE-5	Visitor Control			2.4.5	Visitor Control	CIP 006-3c (R1.4, R1.6)
SG.PE-6	Visitor Records	PE-8	Visitor Access Records	2.4.6	Visitor Records	CIP 006-3c (R1.4, R1.6, R6)
SG.PE-7	Physical Access Log Retention	PE-6	Monitoring Physical Access	2.4.7	Physical Access Log Retention	CIP 006-3c (R7)
SG.PE-8	Emergency Shutoff Protection	PE-10	Emergency Shutoff	2.4.8	Emergency Shutoff	None
SG.PE-9	Emergency Power	PE-11	Emergency Power	2.4.9	Emergency Power	None
SG.PE-10	Delivery and Removal	PE-16	Delivery and Removal	2.4.14	Delivery and Removal	CIP 003-3 (R6) CIP 007-3a (R7, R7.3) CIP 009-3 (R4)
SG.PE-11	Alternate Work Site	PE-17	Alternate Work Site	2.4.15	Alternate Work Site	None

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
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	CIP 006-4c (R2, R7)
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	CIP 003-3 (R1, R2, R3)
SG.PL-2	Smart Grid Information System Security Plan	PL-2	System Security Plan	2.7.2	Control System Security Plan	CIP 003-3 (R4, R4.3)
SG.PL-3	Rules of Behavior	PL-4	Rules of Behavior	2.7.11	Rules of Behavior	CIP 004-3a (R1, R2)
SG.PL-4	Privacy Impact Assessment					None
SG.PL-5	Security-Related Activity Planning			2.7.12	Security-Related Activity Planning	CIP 007-3 (R1, R1.1)
Security Program Management (SG.PM)						
SG.PM-1	Security Policy and Procedures			2.1.1	Security Policies and Procedures	CIP 003-3 (R1, R2, R3, R5, R5.3)
SG.PM-2	Security Program Plan	PM-1	Information Security Program Plan			CIP 003-3 (R2, R2.2, R4.3)
SG.PM-3	Senior Management Authority	PM-2	Senior Information Security Officer			CIP 003-3 (R2)
SG.PM-4	Security Architecture	PM-7	Enterprise Architecture			None
		PL-8	Information Security Architecture			

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.PM-5	Risk Management Strategy	PM-9	Risk Management Strategy			None
SG.PM-6	Security Authorization to Operate Process	PM-10	Security Authorization Process			None
SG.PM-7	Mission/Business Process Definition	PM-11	Mission/Business Process Definition			None
SG.PM-8	Management Accountability	PM-1	Information Security Program Plan	2.2.2	Management Accountability	CIP 003-3 (R2, R3, R5.2)
Personnel Security (SG.PS)						
SG.PS-1	Personnel Security Policy and Procedures	PS-1	Personnel Security Policy and Procedures	2.3.1	Personnel Security Policies and Procedures	CIP 003-3 (R1, R2, R3) CIP 004-3a (R3) CIP 007-3a (R9)
SG.PS-2	Position Categorization	PS-2	Position Risk Designation	2.3.2	Position Categorization	CIP 004-3a (R3)
SG.PS-3	Personnel Screening	PS-3	Personnel Screening	2.3.3	Personnel Screening	CIP 004-3a (R3)
SG.PS-4	Personnel Termination	PS-4	Personnel Termination	2.3.4	Personnel Termination	CIP 004-3a (R4.1, R4.2) CIP 007-3a (R5, R5.2.3)
SG.PS-5	Personnel Transfer	PS-5	Personnel Transfer	2.3.5	Personnel Transfer	CIP 004-3a (R4.1, R4.2) CIP 006-3c (R1.5) CIP 007-3a (R5, R5.1.3, R5.2.3)
SG.PS-6	Access Agreements	PS-6	Access Agreements	2.3.6	Access Agreements	CIP 003-3 (R5.2) CIP 004-3a (R2.1, R4.1) CIP 005-3a (R2.5.3) CIP 006-3c (R1.5, R2, R4)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.PS-7	Contractor and Third Party Personnel Security	PS-7	Third Party Personnel Security	2.3.7	Third Party Security Agreements	CIP 004-3a (R2.1, R3, R4.1)
SG.PS-8	Personnel Accountability	PS-8	Personnel Sanctions	2.3.8	Personnel Accountability	CIP 004-3a (R3, R3.2)
SG.PS-9	Personnel Roles			2.3.9	Personnel Roles	CIP 004-3a (R2, R2.1, R2.2)
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 003-3 (R1, R2, R3, R4.2) CIP 004-3a (R3) CIP 007-3a (R9)
SG.RA-2	Risk Management Plan	PM-9	Risk Management Strategy	2.18.2	Risk Management Plan	CIP 003-3 (R4, R4.1, R4.2, R4.3) CIP 005-3a (R4) CIP 007-3a (R8)
SG.RA-3	Security Impact Level	RA-2	Security Categorization	2.18.8	Security Categorization	CIP 003-3 (R4, R4.1, R4.2, R4.3)
SG.RA-4	Risk Assessment	RA-3	Risk Assessment	2.18.9	Risk Assessment	CIP 003-3 (R6)
SG.RA-5	Risk Assessment Update	RA-3	Risk Assessment	2.18.10	Risk Assessment Update	CIP 003-3 (R3.3) CIP 005-3a (R4.5) CIP 007-3a (R1, R1.3, R2.3, R3.2, R8.4, R9)
SG.RA-6	Vulnerability Assessment and Awareness	RA-5	Vulnerability Scanning	2.18.11	Vulnerability Assessment and Awareness	CIP 003-3 (R6) CIP 005-3a (R4) CIP 007-3a (R2.3, R3.2, R8, R9)
		PM-16	Threat Awareness Program			

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
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	CIP 003-3 (R1, R2, R3) CIP 007-3a (R9)
SG.SA-2	Security Policies for Contractors and Third Parties	PS-7	Third-Party Personnel Security	2.2.5	Security Policies for Third Parties	CIP 004-3a (R2.1, R3, R4.1, R4.2) CIP 007-3a (R5, R5.2.3)
				2.2.6	Termination of Third Party Access	
SG.SA-3	Life-Cycle Support	SA-3	System Development Life Cycle	2.5.3	Life-Cycle Support	None
SG.SA-4	Acquisitions	SA-4	Acquisition Process	2.5.4	Acquisitions	None
SG.SA-5	Smart Grid Information System Documentation	SA-5	Information System Documentation	2.5.5	Control System Documentation	None
SG.SA-6	Software License Usage Restrictions	CM-10	Software Usage Restrictions	2.5.6	Software License Usage Restrictions	None
SG.SA-7	User-Installed Software	CM-11	User-Installed Software	2.5.7	User-installed Software	CIP 007-3a (R3, R5)
SG.SA-8	Security Engineering Principles	SA-8	Security Engineering Principles	2.5.8	Security Engineering Principals	CIP 007-3a (R1, R1.1, R1.2, R1.3)
		SA-13	Trustworthiness			
SG.SA-9	Developer Configuration Management	SA-10	Developer Configuration Management	2.5.10	Vendor Configuration Management	CIP 003-3 (R6)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.SA-10	Developer Security Testing	SA-11	Developer Security Testing and Evaluation	2.5.11	Vendor Security Testing	CIP 007-3a (R1, R1.1 – R1.3)
SG.SA-11	Supply Chain Protection	SA-12	Supply Chain Protection	2.5.12	Vendor Life-cycle Practices	CIP 007-3a (R1, R1.3, R3, R4, R4.2)
Smart Grid Information System and Communication Protection (SG.SC)						
SG.SC-1	Smart Grid 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 003-3 (R1, R2, R3) CIP 005-3a (R1.1 - R1.3) CIP 007-3a (R9)
SG.SC-2	Communications Partitioning			2.8.2	Management Port Partitioning	None
SG.SC-3	Security Function Isolation	SC-3	Security Function Isolation	2.8.3	Security Function Isolation	None
SG.SC-4	Information Remnants	SC-4	Information in Shared Resources	2.8.4	Information Remnants	CIP 007-3a (R7, R7.1, R7.2)
SG.SC-5	Denial-of-Service Protection	SC-5	Denial-of-Service Protection	2.8.5	Denial-of-Service Protection	None
SG.SC-6	Resource Priority	SC-6	Resource Availability	2.8.6	Resource Priority	None
SG.SC-7	Boundary Protection	SC-7	Boundary Protection	2.8.7	Boundary Protection	CIP 005-3a (R1, R1.2, R1.3, R1.6, R2, R2.2, R2.3, R2.4, R3, R3.1, R3.2) CIP 007-3a (R2.1)
SG.SC-8	Communication Integrity	SC-8	Transmission Confidentiality and Integrity	2.8.8	Communication Integrity	None

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.SC-9	Communication Confidentiality	SC-8	Transmission Confidentiality and Integrity	2.8.9	Communication Confidentially	None
SG.SC-10	Trusted Path	SC-11	Trusted Path	2.8.10	Trusted Path	None
SG.SC-11	Cryptographic Key Establishment and Management	SC-12	Cryptographic Key Establishment and Management	2.8.11	Cryptographic Key Establishment and Management	None
SG.SC-12	Use of NIST Approved Cryptography	SC-13	Cryptographic Protection	2.8.12	Use of Validated Cryptography	None
SG.SC-13	Collaborative Computing	SC-15	Collaborative Computing Devices	2.8.13	Collaborative Computing	None
SG.SC-14	Transmission of Security Parameters	SC-16	Transmission of Security Attributes	2.8.14	Transmission of Security Parameters	None
SG.SC-15	Public Key Infrastructure Certificates	SC-17	Public Key Infrastructure Certificates	2.8.15	Public Key Infrastructure Certificates	None
SG.SC-16	Mobile Code	SC-18	Mobile Code	2.8.16	Mobile Code	CIP 007-3a (R4)
SG.SC-17	Voice-Over Internet Protocol	SC-19	Voice Over Internet Protocol	2.8.17	Voice-over-Internet Protocol	None
SG.SC-18	System Connections	CA-3	Information System Connections	2.8.18	System Connections	CIP 005-3a (R1, R1.3, R1.5, R2, R2.2-R2.4, R3, R3.1, R3.2) CIP 006-3c (R1)
SG.SC-19	Security Roles			2.8.19	Security Roles	CIP 003-3 (R5.2)
SG.SC-20	Message Authenticity			2.8.20	Message Authenticity	None

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
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)	None
SG.SC-22	Fail in Known State	SC-24	Fail in Known State	2.8.24	Fail in Know State	None
SG.SC-23	Thin Nodes	SC-25	Thin Nodes	2.8.25	Thin Nodes	None
SG.SC-24	Honeypots	SC-26	Honeypots	2.8.26	Honeypots	None
SG.SC-25	Operating System-Independent Applications	SC-27	Operating System-Independent Applications	2.8.27	Operating System-Independent Applications	None
SG.SC-26	Confidentiality of Information at Rest	SC-28	Confidentiality of Information at Rest	2.8.28	Confidentiality of Information at Rest	None
SG.SC-27	Heterogeneity	SC-29	Heterogeneity	2.8.29	Heterogeneity	None
SG.SC-28	Virtualization Techniques	SC-30	Concealment and Misdriection	2.8.30	Virtualization Techniques	None
SG.SC-29	Application Partitioning	SC-2	Application Partitioning	2.8.32	Application Partitioning	CIP 007-3a (R5.2)
SG.SC-30	Smart Grid Information System Partitioning	SC-32	Information Systems Partitioning			None
Smart Grid Information System and Information Integrity (SG.SI)						
SG.SI-1	Smart Grid 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	CIP 003-3 (R1, R2, R3)
SG.SI-2	Flaw Remediation	SI-2	Flaw Remediation	2.14.2	Flaw Remediation	CIP 003-3 (R6) CIP 005-3a (R4) CIP 007-3a (R3, R3.1, R3.2, R8)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
Smart Grid Cybersecurity Requirement		**NIST SP 800-53 Revision 4**		**DHS Catalog of Control Systems Security: Recommendations for Standards Developers**		**NERC CIPS (1-9) Version 3 October 2010**
SG.SI-3	Malicious Code and Spam Protection	SI-3	Malicious Code Protection	2.14.3	Malicious Code Protection	CIP 007-3a (R4, R4.1, R4.2)
		SI-8	Spam Protection	2.14.8	Spam Protection	CIP 005-3a (R1.5, R3, R3.1, R3.2) CIP 007-3a (R4, R6, R6.1 – R6.5)
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 003-3 (R6) CIP 004-3a (R1)
SG.SI-5	Security Alerts and Advisories	SI-5	Security Alerts, Advisories, and Directives	2.14.5	Security Alerts and Advisories	CIP 003-3 (R1, R2, R3)
SG.SI-6	Security Functionality Verification	SI-6	Security Function Verification	2.14.6	Security Functionality Verification	CIP 003-3 (R4.3) CIP 005-3a (R3.2, R4) CIP 007-3a (R1)
SG.SI-7	Software and Information Integrity	SI-7	Software, Firmware, and Information Integrity	2.14.7	Software and Information Integrity	None
SG.SI-8	Information Input Validation	SI-10	Information Input Validation	2.14.9	Information Input Restrictions	CIP 003-3 (R5)
				2.14.10	Information Input Accuracy, Completeness, Validity and Authenticity	
SG.SI-9	Error Handling	SI-11	Error Handling	2.14.11	Error Handling	None

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 cybersecurity 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 cybersecurity 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[48] 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 to 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,
- Power quality (PQ) harmonics recorders, and

[48] 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.

- 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."[49]) • 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	Smart Grid 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 Validation	• User data protection • Internal system data protection • RBAC

[49] Committee on National Security Systems (CNSS), *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, April 26, 2010, p. 69. http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf [accessed 8/11/2014].

Smart Grid Security Requirement	Smart Grid Requirement Name	Example Security Technologies/Services
		• 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 Restrictions	• Limitation on scope of selectable attributes • Limitation on multiple concurrent sessions • System access banners

Smart Grid Security Requirement	Smart Grid Requirement Name	Example Security Technologies/Services
		• 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

This publication is available free of charge from http://dx.doi.org/10.6028/NIST.IR.7628r1

NISTIR 7628 Revision 1

Guidelines for Smart Grid Cybersecurity

Volume 2 - Privacy and the Smart Grid

The Smart Grid Interoperability Panel –
Smart Grid Cybersecurity Committee

http://dx.doi.org/10.6028/NIST.IR.7628r1

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

NISTIR 7628 Revision 1

Guidelines for Smart Grid Cybersecurity

Volume 2 - Privacy and the Smart Grid

The Smart Grid Interoperability Panel–
Smart Grid Cybersecurity Committee

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.7628r1

September 2014

U. S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology Interagency Report 7628 Rev. 1, Vol. 2
190 pages (September 2014)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: NISTIR.7628.Rev1@nist.gov

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 analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This three-volume report, *Guidelines for Smart Grid Cybersecurity*, presents an analytical framework that organizations can use to develop effective cybersecurity 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 cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

Keywords

advanced metering infrastructure; architecture; cryptography; cybersecurity; electric grid; privacy; security requirements; smart grid

ACKNOWLEDGMENTS

This privacy volume was developed by members of the Smart Grid Interoperability Panel (SGIP) Smart Grid Cybersecurity Committee (SGCC) (formerly the Cyber Security Working Group (CSWG)) Privacy Subgroup. The members of the SGCC Privacy Subgroup come from a wide range of organizations, including some with energy expertise, some with utilities expertise, some with privacy expertise, and some with government expertise, to name just a few of the primary perspectives represented. Special thanks are extended to some of the long-time group members who made exceptional contributions their time and expertise to the group's work products over the years.

- Rebecca Herold (CEO of the Privacy Professor® and Partner, Compliance Helper) has led the SGIP-CSWG Privacy Group since June, 2009. As part of the group activities Rebecca also led the first ever smart grid privacy impact assessment (PIA) in July and August, 2009. She also was an active member of the sub-teams.
- Tanya Brewer of NIST has been the NIST sponsor of the group during this entire time, in addition to being an integral and highly active member of the group, actively contributing to all the sub-teams, coordinating logistics for group meetings, providing insights for scoping issues, along with being the lead editor of this report.
- Amanda Stallings (Ohio Public Utilities Commission (PUC)), has provided extensive time participating in the group's sub-teams, taking meeting notes, and leading a sub-team.
- Brent Struthers (NeuStar) has provided extensive time participating in the group's sub-teams, hosting face-to-face meetings, and leading multiple sub-teams.
- Christine Hertzog (CEO of the Smart Grid Library) has provided extensive time leading the Privacy Use Cases sub-team for the last 2 ½ years of the group's work.
- Sarah Cortes (President, Inman Technology) has provided extensive time leading the sub-team that created, and then updated, the privacy laws section of the report, in addition to being part of the privacy use cases team for 2 ½ years.
- Various representatives of Southern Company contributed significant time and effort during the revision phase of this document and the final development of the privacy use cases.
- We also had some significant contributions from group members for specific topical discussions we've covered over the past three years, with particularly valuable input from Ken Wacks (GridWise Architecture Council), Timothy Schoechle (Smarthome Laboratories, Ltd.), Megan Hertzler (Xcel Energy), and Chris Villarreal (California Public Utilities Commission).

The dedication and commitment of all these individuals over the past four years is significant. In addition, appreciation is extended to all the other group members and various organizations that have committed resources to supporting this endeavor. Members of the CSWG Privacy Subgroup are listed in Appendix K of this report (with the other members of the SGCC). Finally, appreciation and acknowledgment is extended to all the other individuals who have contributed their time and knowledge to ensure this report addresses the privacy needs of the smart grid.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 5
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 Smart Grid Cybersecurity Committee (SGCC) [1] 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 associated risks emerge. Conformance with technical standards does not necessarily result in adequate protections for customer privacy. Privacy is driven by business practices that are supported, but not directed, by technology.

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. NISTIR 7628 does not prescribe public policy with respect to privacy issues. It does, however, explain how technology (such as security tools, e.g., encryption, authorization, and authentication) and internal privacy practices can either enhance or lead to compromises of customer privacy, such as a data breach. Technology choices can complement privacy policies. Privacy impacts and implications may change as the smart grid expands and matures. This chapter addresses residential users and their data. The SGCC Privacy Subgroup will continue to 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 that 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.

[1] The SGIP transitioned to a member-funded non-profit organization in January 2013 and the CSWG was renamed the Smart Grid Cybersecurity Committee (SGCC). For information on the new SGIP organization, see: http://www.sgip.org.

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 may potentially be identified from the signatures they exhibit in electric information at the meter when collections occur with greater frequency, unlike traditional monthly meter readings or smart meter readings that occur once an hour or less frequently.[2] 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 about privacy risks and issues 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 may pose 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, 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 smart grid-related Third Parties.
- Utilities and third-parties providing smart grid products and services need to follow standard privacy and information security practices to effectively and consistently safeguard the privacy of personal information.
- Many consumers may not understand their privacy exposures or their options for mitigating those exposures within the smart grid.
- The consequences of a data breach not only affect the customers whose data may fall into the wrong hands, but may also be costly to smart grid entities. These entities may incur costs to restore the data, to provide compensation such as free credit monitoring for affected customers, to pay any court-awarded damages, and to repair a diminished reputation and loss of corporate good will.
- Privacy protection designed into a system is preferable to a privacy patch or "bolted on" in an attempt to remedy a limitation or omission.

Based on research and the details of the associated findings, a high-level summary listing of all recommendations includes the following points for entities that participate within the smart grid:

[2] K.C. Armel, A. Gupta, G. Shrimali, G., and A. Albert, "Is Disaggregation The Holy Grail of Energy Efficiency? The Case of Electricity," *Energy Policy* 52, January 2013, pp. 213-234. http://dx.doi.org/10.1016/j.enpol.2012.08.062.

- Conduct pre-installation processes and activities for using smart grid technologies with the most transparency possible.
- Conduct an initial privacy impact assessment to understand the current strategy and baseline of privacy risks and benefits before making the decision to invest in and/or install advanced technologies in support of 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 "Consumer-to-Utility PIA Basis and Methodology"). This should include establishing responsibilities for personnel 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.
- Establish processes for de-identifying energy usage data when using aggregated data for activities beyond energy operations for individual customers.
- Educate, through various sources and entities, consumers and other individuals about the privacy risks within the smart grid and what they can do to mitigate them.
- Establish privacy protections for Third Party access to customer energy usage data, in addition to privacy protections related to the commissioning, registration, and enrollment of smart devices with Third Parties.
- Establish information security and privacy protection for wireless transmissions.
- Specific solutions or mitigations for potential electric vehicles/plug-in electric vehicles/plug-in hybrid electric vehicles (generalized as PEVs in this report) privacy issues will need to be explored as technology solutions are deployed going forward. System and infrastructure architects and engineers should, in the meantime, stay aware of potential issues.
- 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

Modernization of the current electric grid through increasing 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 electricity resources in addition to energy produced by power plants (such as renewable energy sources);
- Maintain better reliability in the form of faster and more efficient outage detection and restoration;
- Enable self-healing in cases of disturbance, physical and cyber attack, or natural disaster; and
- Provide customers, and other consumers,[3] 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 energy usage data provided by smart meters, sensors, computer systems, and many other devices to 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 SGCC/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.[4] 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, along with subsequent research activities, 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, government agency representatives, 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

[3] Because customers are often thought of as the individuals who actually pay the energy bills, the SGIP-CSWG Privacy Subgroup determined it was important to include reference to 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 consumers applicable to the situation being described.

[4] This document does not address potential 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. This document in some areas addresses small businesses that would only have one meter and a very small number of employees. This group has previously identified additional potential privacy issues at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/Smart_Grid_Privacy_Groupings_Nov_10_2010_v6.7.xls.

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. The privacy terms used in this chapter are defined in Appendix G.
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, with the exception of retail choice states.[5]
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. **Smart grid data accessed by Third Parties**. Provides privacy protections that organizations who deal directly with energy consumers should implement.
8. **Plug-in electric and plug-in hybrid electric vehicles privacy concerns**. Identifies potential privacy issues and risks related to plug-in electric vehicle communications and provides approaches to mitigate risks.
9. **Smart grid privacy awareness and training**. Explains why providing privacy training and awareness communications to employees and energy consumers is important, and provides links to training slides created to provide train-the-trainer education for those who will be providing smart grid privacy training sessions and modules.
10. **Mitigating privacy concerns with the smart grid and privacy use cases**. Provides a discussion and overview of some existing privacy risk mitigation standards and frameworks. Also includes a description of some methods that can be used to mitigate privacy risks, and points to privacy use cases the group created to help smart grid architects and engineers build privacy protections into the smart grid. The privacy use cases were created by expanding the current collection of SGCC use cases to cover all smart grid value chain participants, in addition to regulated and non-regulated utilities,

[5] "Retail choice states" refers to those states allowing electricity customers the ability to choose their electricity supplier from a variety of electricity service competitors.

that will offer smart grid-related products and services. Developers of smart grid applications, systems, and operational processes can employ a more comprehensive set of privacy use cases, utilizing these cases as a model, to create architectures that build in privacy protections to mitigate identified privacy risks.

11. **Emerging smart grid privacy risks.** Provides brief discussions of fifteen emerging smart grid privacy risks for which organizations and consumers should stay aware.
12. **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.
13. **NIST privacy-related work.** Provides an overview of the National Strategy for Trustworthy Identities in Cyberspace (NSTIC) program and discusses the potential privacy impacts to the smart grid. This section also provides an overview of new NIST work in the area of privacy engineering.
14. **Appendices**. References and additional material.

5.2. WHAT IS PRIVACY?

There is not 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.[6] 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[7] is not the same as confidential information. Confidential information[8] 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.[9]

Additionally, privacy can often be confused with security. Although there may be significant overlap between the two, they are also distinct concepts. There can be security without having privacy, but there cannot be privacy without security; it is one of the elements of privacy. Security involves ensuring the confidentiality, integrity, and availability of data. However, privacy goes beyond having proper authentication and similar security protections. It also addresses such needs as ensuring data is only used for the purpose for which it was collected and properly disposing of that data once it is no longer needed to fulfill that purpose.[10]

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

[6] S.D. Warren and L.D. Brandeis, "The Right to Privacy," *Harvard Law Review* IV(5), December 15, 1890, http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm [accessed 8/11/2014].

[7] See a full definition and discussion of "personal information" in Appendix G.

[8] The use of the phrase "confidential information" in this document does not refer to National Security/classified information.

[9] For example, market data that does not include customer-specific details is considered confidential. Other chapters within this report address confidentiality in depth.

[10] For more on security protections or high-level security requirements, *see* Vol. 1, Chapter 3.

applicable considerations. Data privacy is impacted by the practices of customers who supply personal data and all entities that gather or handle that data.

For example, some have described privacy as consisting of four dimensions:[11]

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 may be created and communicated. For instance, unique electric signatures for consumer electronics and appliances could be compared against some common appliance usage profiles to develop detailed, time-stamped activity reports within personal dwellings. Charging station information might reveal the detailed whereabouts of an electric vehicle/plug-in electric vehicle/plug-in hybrid electric vehicle (generalized as PEVs in this report). This data did not exist before the application of smart grid technologies.[12]

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 and ways to analyze the collected data, which may raise substantial privacy concerns. The reputation of an energy service provider might also be impacted by lapses in customer data privacy protection.

---

[11] *See* Roger Clarke, "What's Privacy?" (August 7, 2006) 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 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.

[12] For instance, consider the enhanced ability the smart grid will give to determining a person's behavior within a premise through more granular energy usage data.

New energy usage data collected outside of smart meters, such as from home energy management systems, 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—

- Identifying potential privacy problems and encouraging the use of relevant Fair Information Practice Principles;[13]
- 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 interests of both smart grid consumers and 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 usage 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 G, and definitions for energy terms are included in Appendix J in Volume 3.

5.3. LEGAL FRAMEWORKS AND CONSIDERATIONS

Since this document was first published in 2010, the legislative frameworks, concepts, and themes have remained generally the same. However, additional smart grid-specific privacy laws and regulations have been passed.[14] Further, an increase[15] during this period in privacy threats

[13] 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. For more information, see §5.9.

[14] In Appendix C, we review at length an example process in which California and Colorado arrived at a legislative and regulatory outcome that may be of use to others in formulating legal and regulatory privacy approaches.

[15] For example, the threat of government surveillance and privacy considerations:

"Seeking Reporters Telephone Records Without Required Approvals", p. 89; "Inaccurate Statements to the Foreign Intelligence Surveillance Court," p. 122; "FBI Issues 11 Improper Blanket NSLs in May to October 2006," p. 165, et al, *A Review of the FBI's Use of Exigent Letters and Other Informal Requests for Telephone Records*, Oversight and Review Division, U.S. Department of Justice, Office of the Inspector General, January 2010. http://www.justice.gov/oig/special/s1001r.pdf [accessed 8/11/2014].

Department of Justice Statistics and reports to Congress on surveillance requests—http://www.justice.gov/criminal/foia/elect-read-room.html [accessed 8/11/2014].

Congressman Markey's Letters to cellphone carriers and their responses with statistical information—http://web.archive.org/web/20130702231920/http://markey.house.gov/content/letters-mobile-carriers-reagrding-use-cell-phone-tracking-law-enforcement [7/2/2013 web snapshot from the Internet Archive Wayback Machine; accessed 8/11/2014].

and public awareness of those threats adds a few considerations to the discussion of legal frameworks and privacy in the smart grid.

Utilities often store Social Security Numbers (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 need to protect not only the items specifically named within existing laws, but in addition to protect energy usage data and associated personal information in ways that existing laws may or may not address.

Generally, privacy concerns include considerations related to the collection and use of energy consumption data. These considerations exist, unrelated to the smart grid, but smart grid aspects fundamentally change their impact.

5.3.1 General Privacy Issues Related to Smart Grid Data

The primary privacy issue related to the deployment of smart grid technologies is that the installation of advanced utility electric meters and associated devices and technology will result in the collection, transmittal and maintenance of personally identifiable data related to the nature and frequency of personal energy consumption and production in a more granular form. This concern arises when this type of data and extrapolations of this data are associated with individual consumers or locations.[16] Utilities have routinely collected energy consumption and personal billing data from customers for decades. The new privacy issues associated with advanced metering infrastructure are related to the behavioral inferences that can be drawn from the energy usage data collected by the meter at more granular frequencies and collected intervals. Additionally, smart meter data also raises potential surveillance issues relating to the methods by which the data is collected and transmitted (electronic collection transmittal rather than manual meter reading and compilation).

The ability to determine specific appliances or customer patterns depends on how often the meter is collecting information and what data the meter is collecting. Collecting energy usage data at more frequent intervals (rather than monthly meter reads using traditional meters) may enable one to infer more information about the activities within a dwelling or other premises than was available in the past.[17] At the time of this report, most residential smart meters in the United States are collecting either 15 minute interval or 1 hour interval consumption data.[18] The data that is measured is total consumption (kWh) during a particular period of time; the availability of

---

Google's disclosure of their own disclosures to law enforcement—http://www.google.com/transparencyreport/userdatarequests/ [accessed 8/11/2014].

Further primary sources of surveillance statistics—http://www.spyingstats.com/ [accessed 8/11/2014].

ACLU summary, "Cell Phone Location Tracking Public Records Request"—http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request [accessed 8/11/2014].

[16] For example, associating pieces of anonymized data with other publicly available non-anonymous data sets may actually reveal information about specific individuals. http://epic.org/privacy/reidentification/ [accessed 8/11/2014]

[17] Smart meter data are not read by the utility in real time, but are accumulated in the meter's memory. (The only exception is pre-pay meters so the customer can be warned when the power will be cut off.) Meters could be programmed to record energy every few seconds, but the internal memory would fill quickly unless the data are sent via the radio to the back office. Frequent data transmissions across a neighborhood area network would require sufficient bandwidth, which inherently has limitations. However, some smart meters can be programmed remotely, so it is possible the frequency of meter reading can be changed after the meter is installed.

[18] Per interviews with subject matter experts conducted at the time of drafting.

that total consumption data over a period of time, combined with the educated knowledge necessary to identify and analyze specific and/or unique appliance/equipment signatures contained within that more granular total consumption data, is what may enable a Third Party to identify particular appliances or usage patterns. The meter itself is only measuring consumption, and any ability to identify specific appliances or usage patterns would require the data to be compared or applied against a pre-determined set of usage patterns or portfolios; the data itself does not identify a specific appliance. The meter may be capable of collecting additional usage information, such as voltage or frequency, but the utility must enable the meter to measure it and make that data available to the utility, customer, or authorized Third Party.

In addition, although many smart meters come pre-equipped with a second radio in order to enable a Home Area Network (HAN), such meters are not necessarily paired with devices installed and located inside a premise by a customer or customer-authorized Third Party by default.[19] When authorized by the utility, the HAN would be allowed to continuously poll the smart meter and obtain data that could continually feed an in-home display with real-time meter information. The connection of a meter to a HAN simply allows for the data to be collected at more frequent intervals, but it is still limited to polling intervals dictated by the meter's technical capability and/or what the meter is set up to provide. If a HAN device is given the polling capabilities of a meter, there could be programs developed to poll a meter for its usage or other readings in a way that may have not been technically enabled by the utility in accordance with the customer's preferences. If so requested or required, one way to minimize the exposure to such programs is to enable all meters to push specific information to a paired HAN device or gateway based on an interval set by the utility or customer. The HAN operators would coordinate with the utility for the initial setup to pair the meter with the HAN using certificates or some form of mutual authentication. Once established, the customer or authorized Third Party would be required to alter the permissions granted to the HAN in order to actively request any additional data from the meter.

With the application of a HAN, it may be possible to access additional information, such as voltage or frequency readings in one-second increments and to identify a particular appliance through data disaggregation of those readings and profiles, provided the utility has activated that ability. Nevertheless, the ability to access this HAN-enabled data is dependent on both the utility enabling this ability and the customer installing the necessary technology. Access to meter data is dependent on the utility. Access to the HAN data is not usually dependent on the utility but rather on the customer's HAN device/system.

Using nonintrusive appliance load monitoring (NALM) techniques, interval energy usage at different time periods can be used to infer individual appliances' portions of energy usage by comparison to libraries of known patterns matched to individual appliances (for an example, see

[19] According to interviews with subject matter experts, in all the known U.S. deployments to date, the smart meter is the network coordinator. Because the smart meter is the network coordinator, for a HAN device to pair to the ZigBee Smart Energy network, the customer would need to provision the HAN device to the smart meter using unique device-specific keys, MAC ID and installation code. The provisioning process may vary depending on the particular smart meter implementation at each utility. For example, in the Texas market, customers, and authorized customer agents (retail electric providers and other Third Parties) are able to provision devices through the use of the Smart Meter Texas web portal. In other areas the provisioning process may be managed through utility-specific portals. Because the customer must first provision the HAN device to the smart meter, it is not currently possible for a HAN device to automatically join the associated smart meter network. And a smart meter that used the Zigbee Smart Energy Profile (SEP) cannot automatically join the customer HAN without the cooperation of the customer. It is important to note that a smart meter isn't necessary for a customer to have a HAN; it is only necessary if the customer wants to access the real-time feed from their associated smart meter.

Figure 5-1 and Figure 5-2). NALM techniques have many beneficial uses for managing energy usage and demand, including pinpointing loads for purposes of load balancing or increasing energy efficiency. However, such detailed information about appliance use has the potential to indicate whether a building is occupied or vacant, show residency patterns over time, and potentially reflect private details of people's lives and activities inside their homes.

The proliferation of smart appliances and devices from entities other than utilities throughout the smart grid means an increase in the number of devices that may generate data beyond the utility's metering and billing systems. This data may also be outside the utility's responsibility. The privacy issues presented by the increase in these smart appliances and devices on the consumer side of the meter are expanded if such appliances and devices transmit data outside of the HAN or energy management system (EMS) and do not have documented security requirements (e.g., a smart appliance being able to send data back to the manufacturer via telematics), thereby effectively extending the reach of the system beyond the walls of the premises. An additional consideration is that new Third Party entities may also seek to collect, access, and use energy usage data directly from customers, rather than from the utility (e.g., vendors creating energy efficiency or demand response applications and services specifically for smart appliances, smart meters, and other building-based solutions). The ability of the customer to understand these risks may require customers to be better educated and informed on the privacy consequences of decisions regarding these Third Party services. However, customer education is not the only method to address Third Party access challenges. There is also a need to develop guidance that both service providers and Third Parties can leverage to conduct privacy risk analyses and explore mitigation options, which may include establishing effective default privacy settings, clear user interfaces, improved educational outreach to ensure that customers are fully aware and consent to Third Parties' use of their information, and establishing or pointing to existing privacy standards for Third Parties to use.

An additional issue is that as smart grid technologies collect more detailed data about households, law enforcement requests to access that data for criminal investigations may include requests for this more detailed energy usage data, which heretofore has generally been neither of interest nor use to law enforcement. Law enforcement agencies have already used monthly electricity consumption data in criminal investigations. For example, in *Kyllo* v. *United States*, 533 U.S. 27 (2001), the government relied on monthly electrical utility records to develop its case against a suspected marijuana grower.[20]

Unlike the traditional energy grid, the smart grid may be viewed by some as carrying private and/or confidential electronic communications between utilities and end-users, possibly between utilities and Third Parties, 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.[21] Law enforcement agencies may have an interest in establishing or confirming presence at an address or location at a certain critical time, or possibly establishing certain

[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), 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. For more, *see* §5.3.2.2.

[21] See, e.g., Electronic Communications Privacy Act, 18 U.S.C. § 2510. http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html [accessed 8/11/2014].

activities within the home —information that may be readily obtained from energy usage data collected, stored, and transmitted by new, more granular smart grid technologies, such as a HAN that accesses a smart meter capable of a real-time feed. Accordingly, these types of situations regarding smart grid data warrant review and consideration in comparison to similar restrictions on law enforcement access to other personal and private information under existing constitutional and statutory privacy requirements.[22]

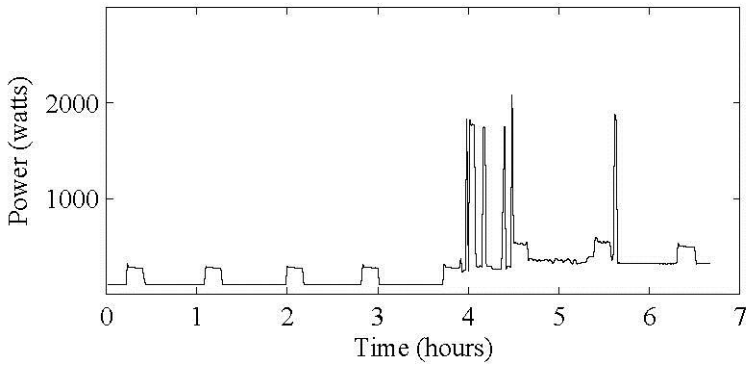
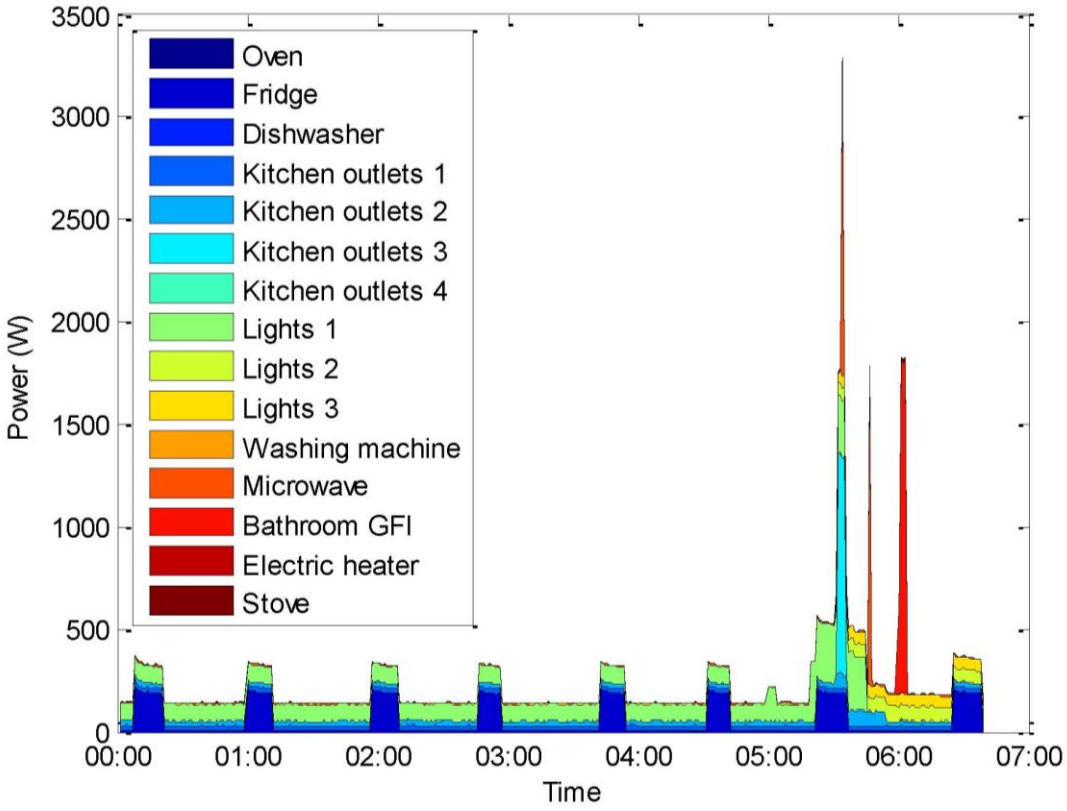


Figure 5-1 Meter Data Collected at 1 Minute Intervals[23]



[22] For example *Kyllo* demonstrates that some subpoenas are illegal, whereas others are not. See also *Golden Valley*, p. 8. *See* footnote 26 for full reference for *Golden Valley*.

[23] O. Parson, S. Ghosh, M. Weal, and A. Rogers, "Non-intrusive Load Monitoring using Prior Models of General Appliance Types [extended abstract]," *1st International Workshop on Non-Intrusive Load Monitoring*, Pittsburgh, Pennsylvania, May 7, 2012, http://www.ices.cmu.edu/psii/nilm/abstracts/parson_Southampton_NILM2012_abstract.pdf [accessed 8/11/2014].

Figure 5-2 Using Hidden Markov Models (HMM) to Produce an Appliance Disaggregation[24]

5.3.2 Existing Legal and Regulatory Frameworks

When considering the possible legal issues relating to smart grid privacy, it is important to note that general privacy laws currently in effect may or may not already apply to personal information generated by the smart grid even if the laws do not explicitly reference the smart grid (including unique smart grid data and/or technology). On the other hand, existing state-level smart grid and electricity delivery regulations may or may not explicitly reference privacy protections.

While it is uncertain how general privacy laws may or may not apply to energy usage data collected, stored, and transmitted by smart grid technologies, it is clear that the smart grid brings new challenges and privacy issues, which can lead to detailed information and additional insights about device usage, including medical devices and vehicle charging data that may be generated by new services and applications provided directly by third-parties to customers.[25] These new data items, and new uses of existing data may require additional study and public input to adapt to current laws or to shape new laws and regulations.

To understand the types of data items that may be protected within the smart grid by existing non-smart grid-specific privacy laws and regulations it is important to first consider some of the most prominent examples of existing laws and regulations that provide for privacy protection, which will be discussed in the following sections.

5.3.2.1 Overview of U.S. legal privacy protection approaches

There are generally four approaches in the U.S. to protecting privacy by law—

- **Constitutional Protections and Issues: General protections**. The First (freedom of speech), Fourth (search & seizure), Fifth (self-incrimination), and Fourteenth Amendments (equal protection), cover personal communications and activities.
- **Statutory, Regulatory and Case Law, both Federal and State**
- **Data-specific or technology-specific protections, including direct regulation of public utilities by state public utility commissions**. These protect specific information items such as credit card numbers and Social Security Numbers (SSN); or specific technologies such as phones or computers used for data storage or communication; or customer-specific billing and energy usage information used by public utilities to provide utility services. Other federal or state laws or regulations may apply privacy protections to information within the context of specific industries (e.g., Gramm-Leach-Bliley, Health Insurance Portability and Accountability Act (HIPAA), etc.).
- **Contractual and Agreement-related Protections and Issues: Specific protections**. These are protections specifically outlined within a wide range of business contracts, such as those between consumers and businesses.

[24] *Ibid.*

[25] For additional possible privacy concerns in different scenarios and settings, refer to the Privacy Subgroup's Privacy Matrix—http://collaborate.nist.gov/twikisggrid/pub/SmartGrid/CSCTGPrivacy/Smart_Grid_Privacy_Groupings_Nov_10_2010_v6.7.xls [accessed 8/11/2014].

Even though some states and public utilities commissions (PUCs) have laws and/or regulations in place to protect energy consumption data in some manner, some states, such as California and Colorado, have passed or implemented rules and regulations specifically focused on the energy consumption data produced by smart meters. Energy consumption patterns have historically not risen to the level of public concern given to financial or health data because (1) electric 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 could not be analyzed to reveal usage by specific appliance, and (3) it was not possible or as easy for utilities to share this specific granular 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 may reveal personal activities and the use of specific energy using or generating appliances[26], and because the data can 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. However, state PUCs may be able to assert jurisdiction over utility privacy policies and practices because of their traditional jurisdiction and authority over the utility-retail customer relationship.[27]

5.3.2.2 Constitutional Protections and Considerations

Fourth Amendment Search and seizure considerations, Warrants and Subpoenas

Fourth Amendment provisions, pertaining to unreasonable search & seizure, have been applied to the ways government officials have attempted to obtain energy consumption data, although the ways in which utilities collect the data, such as through meters, is not at issue in such cases. In *Kyllo*, U.S. law enforcement's warrantless use of thermal imaging technology to monitor energy consumption was found to be an unlawful "search" under the Fourth Amendment.

How the Fourth Amendment might further apply to data collected about appliances and patterns of energy consumption, to the extent that energy usage data collected, stored, and transmitted by smart grid technologies reveals information about personal activities is yet to be determined.

Not all subpoenas, although issued by the US government and approved by a court, may be lawful. Higher courts have repeatedly found subpoenas issued by lower courts to be unlawful. Partially due to legal challenges to subpoenas, it may sometimes be unclear to smart grid service providers whether to comply with subpoenas or to appeal them to higher courts. This is a subject of the *Golden Valley*[28] decision.

[26] For more discussion on this, see §5.3.1

[27] For more information about how California and Colorado instituted their relevant rules, *see* Appendix C: Changing Regulatory Frameworks.

[28] *UNITED STATES OF AMERICA*, v. *GOLDEN VALLEY ELECTRIC ASSOCIATION*, Case No. 11-35195 (C.A. 9 2012), http://www.ca9.uscourts.gov/datastore/opinions/2012/08/07/11-35195.pdf [accessed 8/11/2014].

CALEA and Subpoenas (Data already collected and stored by Third Parties)

The Communications Assistance for Law Enforcement Act (CALEA) details how the U.S. government may obtain telecommunications and location data from telecommunications service providers through subpoenas without a Fourth Amendment violation. Under CALEA, the government may not compel Third Party communications service providers to collect data they would not otherwise collect. However, if they are already collecting and storing it, CALEA allows the government to compel them to hand it over. Thus, service providers must now consider carefully whether to collect "unnecessary" data which may seem interesting, but which may later expose consumers to privacy risks. It has not yet been determined by the courts if smart meters do or do not qualify as "telecommunications devices" for the purposes of CALEA.

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. Data ownership is a very complex issue that may be viewed as a question of who should have what rights to the data. (e.g., right to control, right to exclude, etc.) These rights may be divided or shared among multiple entities. Alternatively, entities that have the ability to control or manage the data may have some responsibilities regarding the data, regardless of "ownership." Data ownership is an issue touched upon in the *Golden Valley* case discussed below under Case Law (§5.3.2.4).

National Security Letters

In 1994, an amendment to the Foreign Intelligence Surveillance Act of 1978 (FISA)[29] introduced National Security Letters ("NSLs"), broadening the government's scope in obtaining information relating to terrorist investigations without judicial oversight, in narrow circumstances. However, the power granted under FISA for these NSLs was significantly expanded in 2005. Since that time, constitutional challenges to NSLs have increased, again leaving "gray areas" when it comes to service providers' compliance.

Evidence and reporting of NSL abuse started in 2005, when the U.S. Department of Justice (DOJ) Inspector General's Office found widespread abuse. The *Washington Post* reported in 2010 that the "FBI illegally collected more than 2000 U.S. telephone call records," using methods that FBI general counsel Valerie Caproni admitted "technically violated the Electronic Communications in Privacy Act when agents invoked nonexistent emergencies to collect records."[30] The FBI admitted that "about half of the 4400 toll records collected in emergency situations... were done in technical violation of the law," and that "agents broadened their searches to gather numbers two and three degrees of separation from the original request." By October, 2013, 39 companies, including Google, Microsoft, Apple, Facebook, and Twitter, and 51 non-governmental organizations (NGOs), including the American Civil Liberties Union and Electronic Frontier Foundation (EFF), had signed a letter to President Obama protesting the gag NSLs ordered on their own and others' reporting, and urging

[29] *Foreign Intelligence Surveillance Act of 1978* ("FISA"; Pub.L. 95-511, 92 Stat. 1783, enacted October 25, 1978, 50 U.S.C. ch.36, S. 1566)

[30] J. Solomon and C. Johnson,"FBI broke law for years in phone record searches," *Washington Post*, January 19, 2010; A01 http://www.washingtonpost.com/wp-dyn/content/article/2010/01/18/AR2010011803982_pf.html [accessed 8/11/2014].

immediate and specific reforms.[31] "Basic information about how the government uses its various law enforcement–related investigative authorities has been published for years without any apparent disruption to criminal investigations," the letter noted. Recently, in March 2013, EFF won a landmark decision entitled *In Re National Security Letter* in the Northern District of California in which Judge Susan Illston declared one of the NSL statutes unconstitutional in its entirety.[32] It was noted that a judge may eliminate the gag order that an NSL carries only if they have "no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal counter-terrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person."[33] Most recently, several companies have been able to publish more accurate data on the number of NSLs and FISA court requests they have received in recent years, showing "a spike of affected accounts" between July and December 2012.[34]

5.3.2.3 U.S. Federal Privacy Laws and Regulations

U.S. federal privacy laws cover a wide range of industries and topics. It is currently not clear to what extent the following laws that provide privacy protections may apply, if at all, to the more revealing uses of consumer energy usage data that may be made possible by advanced smart grid technologies and identification techniques.[35]

- Healthcare: Examples include the Health Insurance Portability and Accountability Act (HIPAA) and the associated Health Information Technology for Economic and Clinical Health (HITECH) Act.
- Financial: Examples include the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transactions Act (FACTA), and the Equal Credit Opportunity Act (ECOA).
- Education: Examples include the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA).
- Communications: Examples include the First Amendment to the U.S. Constitution, the Electronic Communications Privacy Act (ECPA), and the Telephone Consumer Protection Act (TCPA).

---

[31] "We, the undersigned, are writing to urge greater transparency around national security-related requests by the US government to Internet, telephone, and web-based service providers", July 18- September 30, 2013, https://www.cdt.org/files/pdfs/weneedtoknow-transparency-letter.pdf [accessed 8/11/2014].

[32] M. Zimmerman, "In Depth: The District Court's Remarkable Order Striking Down the NSL Statute," *Electronic Frontier Foundation* [Web site], March 18, 2013, https://www.eff.org/deeplinks/2013/03/depth-judge-illstons-remarkable-order-striking-down-nsl-statute [accessed 8/11/2014].

And see Hon. S. Illston, "In Re National Security Letter," March 14, 2013, https://www.eff.org/sites/default/files/filenode/nsl_order_scan.pdf [accessed 8/11/2014].

[33] P. Elias, "National Security Letters Unconstitutional, Rules Judge," *The Huffington Post*, March 16, 2013, http://www.huffingtonpost.com/2013/03/16/national-security-letters_n_2892568.html [accessed 8/11/2014].

[34] S. Rosenblatt, "Tech firms reveal even more about FISA requests," *CNET*, February 3, 2014, http://news.cnet.com/8301-1009_3-57618266-83/tech-firms-reveal-even-more-about-fisa-requests/ [accessed 8/11/2014].

[35] As of May 28, 2013, there was only one adjudicated U.S. case related to privacy and energy usage data, *Friedman* v. *Maine PUC*.

- Government: Examples include the Privacy Act of 1974, the Computer Security Act of 1987, and the E-Government Act of 2002.
- 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").
- Privacy in the Home: Examples are the protections provided by the Fourth, Fifth, and Fourteenth Amendments to the U.S. Constitution.
- Employee and Labor Laws: Examples include the Americans with Disabilities Act (ADA) and the Equal Employment Opportunity (EEO) Act.
- General Business and Commerce: One example is Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices, and has been used by the FTC to cover a wide variety of businesses.

5.3.2.4 State Privacy Laws and Regulations: Smart Grid-Specific

In 2012, according to the National Conference of State Legislatures,[36] "at least 13 states" (California, Illinois, Massachusetts, Maine, Michigan, New Hampshire, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island and Vermont) took up consideration of 31 smart grid-specific bills. Several of these laws supplement pre-existing utility laws or regulations that already are intended to protected customer-specific information collected by utilities, such as billing and credit information, from unauthorized disclosure except where specifically required for purposes such as utility services, equal access by non-utility retail energy providers, or law enforcement pursuant to valid subpoenas.[37] The following seven States have enacted smart grid-specific privacy protection laws:

- California Senate Bill 1476 – customer data generated by smart meters is private and can only be shared with Third Parties upon consent of the customer, with the following exceptions: for basic utility purposes, at the direction of the California PUC, or to utility contractors implementing demand response, energy efficiency or energy management programs;
- Illinois S.B. 1652 - develop and implement an advanced smart grid metering deployment plan, which included the creation of a Smart Grid Advisory Council and H.B. 3036 Amended the smart grid infrastructure investment program and the Smart Grid Advisory Council;
- Maine H.B. 563 – directed the Public Utility Commission to investigate current cybersecurity and privacy issues related to smart meters;

[36] J. Pless, "2012 Smart Grid State Action," National Conference of State Legislatures [Web site], July 9, 2012, http://www.ncsl.org/research/energy/smart-grid-state-action-update.aspx [accessed 8/11/2014].

[37] See, e.g. California Public Utilities Commission Decision No. 11-07-056, Attachment B, "List of Current Statutes, Regulations, Decisions and Protocols Related to Customer Privacy Applicable to California Energy Utilities," July 28, 2011, http://docs.cpuc.ca.gov/PublishedDocs/PUBLISHED/GRAPHICS/140370.PDF [accessed 8/11/2014].

- New Hampshire - S.B. 266 prohibition on utility installation of smart meters without the property owners' consent. Utilities must disclose in writing the installation of a smart meter;
- Ohio S.B. 315 – encourages innovation and market access for cost effective smart grid programs and H.B. 331 – creates a Cybersecurity, Education and Economic Development Council to help improve state infrastructure for cybersecurity;
- Oklahoma Law H.B. 1079 – established the Electronic Usage Data Protection Act that directs utilities to provide customers with access to and protection of smart grid consumer data;
- Vermont S.B. 78 – promote statewide smart grid deployment and S.B. 214/Act 170 – directs the Public Utility Board to set terms and conditions for access to wireless smart meters. The law also requires consumers' written consent prior to smart meter installation and requires removal of smart meters upon request/cost-free opt-out of Smart Meters.

U.S. Case Law Relevant to the Smart Grid

Two U.S. cases have recently been decided applying to energy consumption data and evolving technology, joining *Kyllo*:

- *US* v. *Golden Valley*- US 9th Circuit[38] - 8/7/12
- *Friedman* v. *Maine PUC* - Supreme Court of Maine[39]- 7/12/12

In *Golden Valley*, a non-profit rural electric cooperative lost an appeal in the 9th Circuit federal court, and was required to comply with an administrative subpoena to provide consumer records pursuant to a DEA investigation. Golden Valley opposed the petition, primarily relying on a company policy of protecting the confidentiality of its members' records. The district court granted the petition to enforce the subpoena. Golden Valley complied but appealed the subpoena, which it felt was unlawful, on the grounds that it was:

- Irrelevant to the investigation;
- Inadequately following DEA and judicial oversight procedures; was an administrative subpoena with a lower burden of cause;
- Overbroad; and
- Violating 4th amendment search and seizure principles.

Golden Valley Electric Association argued that fluctuating energy consumption is "not unusual" in its area and so "not obviously relevant" to a drug crime. The Ninth Circuit rejected Golden Valley's arguments, upholding the district court order enforcing the subpoena. The Court referenced a view that consumers do not own their own energy consumption data. This view is based on the contract which consumer signs, allowing the utility use of the data. Other opinions, however, have disagreed with this approach, arguing it significantly erodes privacy. For

[38] See Footnote 26 for full citation.

[39] *ED FRIEDMAN et al*. v. *PUBLIC UTILITIES COMMISSION et al.*, PUC-11-532 (S. CT MAINE 2012), http://www.courts.state.me.us/opinions_orders/supreme/lawcourt/2012/12me90fr.pdf [accessed 8/11/2014].

example, earlier this year, Supreme Court Justice Sotomayor noted in her concurring opinion[40] in *United States* v. *Jones*, a case dealing with GPS data, that the elimination of privacy rights in information voluntarily turned over to Third Parties is "ill-suited for the digital age we live in today."

Although it ruled against Golden Valley, the 9th Circuit indicated a possible new legal approach. Specifically, the court said that in some circumstances "a company's guarantee to its customers that it will safeguard the privacy of their records might suffice to justify resisting an administrative subpoena."[41] The Court did note that the outcome might have been different if Golden Valley had entered into a contract with its customers specifically agreeing to keep such business records confidential.[42]

In 2012, the first court case discussing privacy in the context of the smart grid was tried in the Maine Supreme Court. In *Friedman*, the Maine Supreme Court partially invalidated the Maine Public Utilities Commission's ("Maine PUC") dismissal of plaintiff Friedman's objections to a Smart Meter opt-out penalty. First, the court rejected the Maine PUC's arguments that Friedman's health and safety concerns had been "resolved" by its opt-out investigations in another proceeding, because the Commission had explicitly declined in those proceedings to make any determination on health and safety -- instead deferring to the jurisdiction of the Federal Communications Commission (FCC). The court held the Maine PUC could not explicitly decline to make determinations on health and safety in the opt-out investigations proceedings, and then attempt to treat the issues as "resolved" in this proceeding. Having never determined whether the smart-meter technology is safe, it could not conclude whether the opt-out fee was "unreasonable or unjustly discriminatory."

Second, the Maine Supreme Court concluded that the Maine PUC had resolved the privacy, trespass, and Fourth Amendment claims against the utility, but did not state exactly how the Maine PUC concluded that was the case.

Finally, the Maine Supreme Court also affirmed that the plaintiffs' constitutional Fourth and Fifth Amendment claims brought against the Maine PUC were properly dismissed as without merit. Therefore, the Maine Supreme Court invalidated the portion of the Maine PUC's decision regarding health and safety, remanding it back to the Maine PUC for further proceedings to resolve that issue, and otherwise affirmed the rest of its decision.

5.3.2.5 Contractual Approaches and Issues Related to Consumer Agreements

Opt-Out Provisions

In response to both potential privacy and health concerns, some state legislatures and regulatory commissions have required that the customer be given the option to opt-out of smart meter implementation as part of a contract for service with a utility, or to have an installed smart meter

[40] *United States v. Jones*, 565 US ___, 132 S.Ct. 945 (2012), p. 3 (Justice Sotomayor's concurring opinion https://www.eff.org/node/69475, p.5).

[41] Golden Valley, 8922.

[42] Golden Valley, 8922.

removed.[43] Additionally, some utilities have voluntarily offered this option for their customers.[44] The *Friedman* case discussed above reviewed the procedural grounds for a Maine PUC decision regarding proposed opt-out provisions.

5.3.3 Applicability of Existing Data Protection Laws and Regulations to the Smart Grid

Personally identifiable information (PII) has no single, authoritative, legal definition. Fair Information Practice Principles (FIPPs) provide the most generally accepted, rather than legal, definition. However, as noted in above, 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 HIPAA, 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. In 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.[45] This is an example of how a federal law regarding one industry (i.e., healthcare) has been generally adopted at the state level as a law to protect the information of citizens (in this case, health information) regardless of the industry of organizations handling that information.

Private industry's definition of personally identifiable information predates legislation and is generally legally defined[46] 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,[47] 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:

---

[43] N.H. Rev. Ann. Stat. § 374:62 (prohibiting electric utilities from installing and maintaining smart meter gateway devices without a property owner's consent); Vt. Stat. Ann. tit. 30, § 8001 (requiring public service board to establish terms and conditions governing the installation of wireless smart meters). See also, Nev. P.S.C. Case 11-10007 (February 29, 2012) (adopting recommendation that Nevada Energy provide opt-out opportunity for residential customers); and Texas P.U.C. Case 40199 (May 17, 2012) (refusing to initiate rulemaking requiring opt-out options for smart meter deployment).

[44] See Cal. P.U.C. Case No. A. 11-03-014 (February 1, 2012) (approving Pacific Gas & Electric's SmartMeter program, allowing residential customers to opt-out of smart meter deployment); Pursuing the Smart Meter Initiative, Me. P.U.C. Docket No. 2010-345 (May 19, 2011) (approving Central Maine Power's customer opt-out program); P.S.B. Vt. Tariff 8317 (March 8, 2012) (approving Central Vermont Public Service Smart Power Wireless Meter Opt-Out tariff); and P.S.B. Vt. Tariff 9298 (March 8, 2012) (approving Green Mountain Power smart meter opt-out policy).

[45] 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 in P. MacKoul, "Impact of the Attorney General Opinion GA-0519 on Medical Information & HIPAA," 2007, http://www.hipaasolutions.org/white_papers/HIPAA%20Solutions,%20LC%20White%20Paper%20-Texas%20AG%20Opinion%20On%20Privacy%20And%20HIPAA.pdf [accessed 8/11/2014].

[46] For example, most of the U.S. state breach notice laws define personal information to be first name or first initial and last name in combination with any one or more of other specified data elements. See a listing of the laws, with links to the regulatory text, at "Security Breach Notification Laws" (National Conference of State Legislatures), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, [accessed 8/11/2014].

[47] See text of the Massachusetts breach notice law, "An Act Relative to Security Freezes and Notification of Data Breaches," *Chapter 82*, 2007, http://www.mass.gov/legis/laws/seslaw07/sl070082.htm [accessed 8/11/2014].

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number.

As noted at the outset of Section 5.3 above, businesses often store SSNs and financial account numbers in their payroll or billing systems. For instance, utilities have been obligated to follow the associated legal requirements for safeguarding this data for many years. For all organizations that handle energy usage data, the sharing and storage capabilities that the smart grid network brings to bear creates the need to protect not only the items specifically named within existing laws, but in addition to protect new types of personal information that are created using smart grid data.

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 revealed by the privacy impact assessment (PIA) found in Section 5.4, there may be a lack of privacy laws or policies directly applicable to the smart grid. Privacy subgroup research indicates that, in general, many state utility commissions currently lack formal privacy policies or standards related to the smart grid.[48] 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. However, existing privacy laws and regulations regarding consumer usage information may or may not be applicable to energy usage information related to smart grid technologies. These laws and regulations may not be applicable if a customer shares its information with organizations other than utilities.

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 analysis aimed at determining how collected data can reveal personal information about individuals or groups of individuals. The scope of the PIA can vary from the entire grid to a segment within the grid. Privacy risks 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: (1) determining the types of information that may be collected or created that can then reveal information about individuals or activities within specific premises (primarily residential); (2) determining how these different types of information may be exploited; and (3) recommending business/organization information security and privacy policies and practices to mitigate the identified privacy risks. Entities of all types

[48] Most public utility commissions have significant customer privacy policies that predate the smart grid. It is not clear whether and to what extent these privacy policies would apply to smart grid data, or the extent to which they would need to be updated to reflect the new uses of smart grid data as they affect these traditional privacy issues.

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 that are part 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 privacy practice standards 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)[49] 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 FIPPs, also often called "Privacy Principles," that are the framework for many modern privacy laws around the world. Several 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),[50] the Organisation for Economic Cooperation and Development (OECD) Privacy Principles, and information security management principles from the International Organization for Standardization (ISO) and

[49] *See* "AMI Systems Use Cases" at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/AugustWorkshop/All_of_the_Diagrams_in_one_document.pdf [accessed 8/11/2014].

[50] *See* D. Cornelius,"AICPA's Generally Accepted Privacy Principles," *Compliance Building* [Web site], January 9, 2009, http://www.compliancebuilding.com/2009/01/09/aicpas-generally-accepted-privacy-principles/ [accessed 8/11/2014].

International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) *International Standard ISO/IEC 27001*[51] as its primary evaluation criteria:[52]

- 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*,[53] 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*,[54] wherein paragraphs 7–14 of Part Two[55] outline the basic principles of national application, and on the "Explanatory Memorandum,"[56] wherein those principles are amplified (by paragraph number) in subsection II.B.[57] 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 the OECD privacy principles.[58][59]

---

[51] *See* International Standards Organization/International Electrotechnical Commission, *Information technology—Security techniques—Information security management system—Requirements*, ISO/IEC 27001:2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534 [accessed 8/11/2014].

[52] Since the PIA was conducted in 2009, more documents have been published that may be useful in conducting a PIA. Two of these are the Consumer Privacy Bill of Rights (Feb 2012) and NIST Special Publication 800-53 Revision 4 Appendix J (Apr 2013, including updates as of 1/15/2014).

[53] The *Guidelines* document has since been added to the OECD's 2013 Privacy Guidelines. *See* http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines [accessed 8/11/2014].

[54] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#guidelines [accessed 8/11/2014].

[55] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2 [accessed 8/11/2014].

[56] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#memorandum [accessed 8/11/2014].

[57] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#comments [accessed 8/11/2014].

[58] Per the *OECD Privacy Principles*, http://oecdprivacy.org/, "Internationally, the OECD Privacy Principles provide the most commonly used privacy framework, they are reflected in existing and emerging privacy and data protection laws, and serve as the basis for the creation of leading practice privacy programs and additional principles."

[59] Alternatively, one could use the Fair Information Practice Principles (FIPPs) found in Appendix A of the *National Strategy for Trusted Identities in Cyberspace*, developed since the original issuance of this document. Appendix A is available at: http://www.nist.gov/nstic/NSTIC-FIPPs.pdf [accessed 8/11/2014]. Rooted in the United States Department of Health, Education and Welfare's seminal 1973 report, "Records, Computers and the Rights of Citizens" (1973), these principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as in those of many foreign nations and international organizations. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies.

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 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,[60] 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 protecting smart grid data. Organizations can also use the six questions listed in Section 5.4 when conducting their own PIAs and then examine their findings with the ten privacy principles listed in Appendix F. 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 associated with the use of smart grid data in new ways that can cause privacy concerns. 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 PIA Findings and Recommendations Summary of the Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment[61] used the privacy principles as the basis for the PIA. Within the summary, each 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.

Privacy Practices Recommendations:

- **Policy challenge procedures**. Organizations collecting energy data, and all other entities with access to that data, 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

[60] *See* 5.3.2, Existing Legal and Regulatory Frameworks, and 5.3.3, Applicability of Existing Data Protection Laws and Regulations to the Smart Grid.

[61] See the summary of the Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment in Appendix F. See the full "NIST Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment," September 10, 2009, at https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/NIST_High_Level_PIA_Report_FINAL_-_Herold_Sept_10_2009.pdf. [accessed 8/11/2014].

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 the PIA results for review by an impartial Third Party and making a summary of the results available to the 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 or amend policies and procedures to identify breaches and misuse of the 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 consumer data 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 shown in the PIA, 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 lifestyle of residential consumers and the business operations of commercial and industrial consumers.[62]

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, it has been shown through multiple research studies[63] and incidents[64] that a piece of

[62] The ability to determine personal activities according to energy consumption data alone was demonstrated recently in quotes from a Siemens representative in a Reuters news article: "We, Siemens, have the technology to record it (energy consumption) every minute, second, microsecond, more or less live," said Martin 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 [accessed 8/11/2014].

[63] *See* A. Narayanan and V. Shmatikov, "Myths and Fallacies of 'Personally Identifiable Information'," *Communications of the ACM* 53(6), June 2010, pp. 24-26, http://dx.doi.org/10.1145/1743546.1743558. 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.

[64] 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

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 potential matches to an individual may be narrowed because of situational circumstances to the point that linking becomes an easy task.[65] (This may particularly be seen in sparsely populated geographical areas or for premises with unique characteristics.)

Another study published in 2009 illustrates the increasing ease of disaggregating 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.[66]

There are potential unintended consequences of seemingly anonymous smart grid data being compiled, stored, and cross-linked. 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[67] 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[68] activities.

Table 5-1 identifies and describes potential data elements within the smart grid that could impact privacy if not properly safeguarded. This is not an exhaustive list of all data elements about customers that could pose a privacy risk. There is additional risk outside of the smart grid around the access of certain data elements.

---

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* M. Barbaro and T. Zeller, Jr., "A Face is Exposed for AOL Searcher No. 4417749," *The New York Times*, August 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000 [accessed 8/11/2014].

[65] L. Sweeney, "k-anonymity: A Model for Protecting Privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems* 10(5), October 2002, pp. 557-570, http://dx.doi.org/10.1142/S0218488502001648. 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.

[66] A. Acquisti and R. Gross, "Predicting Social Security numbers from public data," *PNAS: Proceedings of the National Academy of Sciences* 106(27), July 7, 2009, pp. 10975-10980, http://dx.doi.org/10.1073/pnas.0904891106.

[67] 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.

[68] 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.

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 provided
Account Number	Unique identifier for the account
Meter reading	kWh energy consumption recorded between 15 to 60 minute intervals and once daily intervals during the current billing cycle
Financial information	Current or past meter reads, bills, and balances available, including history of late payments/failure to pay, if any
Lifestyle	When the home is occupied and unoccupied, when occupants are awake and asleep, how much various appliances are used[69]
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 Unique Identifiers	The Internet Protocol (IP) address, media access control (MAC) address, or other network identifiers for the meter, if applicable

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:

Category 1: Personal information not previously readily obtainable; and

Category 2: Mechanisms that did not previously exist for obtaining (or manipulating) personal information.

Examples of the first category 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.

The second category includes instances where personal information is available from other sources, and the smart grid may present a new source for that same information. For example, an individual's physical location can be tracked through their credit card and cell phone records today. Charging PEVs raises the possibility of tracking physical location through new energy consumption data.

[69] For discussion on this topic, see §5.3.1.

Detailed profiles of activities within a house or building can be derived from "equipment electricity signatures"[70] and their time patterns. Such signatures and patterns can provide a basis for making assumptions about occupant activities (e.g., when the premise was unoccupied).[71]

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 categories given above. While this is not an exhaustive list, it serves to help categorize the concerns noted.

Table 5-2 Potential Privacy Concerns and Descriptions

Privacy Concern	Discussion	Categorization Category 1: Personal information not previously readily obtainable. Category 2: Mechanisms that did not previously exist for obtaining (or manipulating) personal information.
Personal data exposure	Unauthorized exposure of energy consumption or other personal information.	Category 2: The traditional method of reading consumer meters (either manual recording or electronically via "drive-by" remote meter reading systems) may allow less opportunity for data manipulation or exposure without collusion with the personnel handling the data.
Determine Personal Behavior Patterns / Appliances Used	Smart meters, combined with home automation networks or other enabling technologies, 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[72]. Possible uses for this information include: • Appliance manufacturers product reliability and warranty purposes; • Targeted marketing.	Category 1: The type of data made available by smart grid implementation may be both more granular and available on a broader scale.

[70] This is a term coined by the Privacy Subgroup and not one that is officially used by any regulatory or standards group.

[71] While using NALM techniques to compare appliance signatures against total consumption data can provide a basis for assumptions regarding the number of individuals in a given location, such techniques cannot conclusively reveal the number of individuals in a location. For example, even if NALM techniques can reveal that a toaster (or hot water heater) was used at 8am, 10am, and 12noon, it cannot distinguish between 3 toast-eaters (or shower-takers) and 1 toast- (or shower-) loving person.

[72] For discussion on this topic, see §5.1.

Privacy Concern	Discussion	Categorization Category 1: Personal information not previously readily obtainable. Category 2: Mechanisms that did not previously exist for obtaining (or manipulating) personal information.
Perform Real-Time Remote Surveillance	Access to live energy use data can potentially 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.	Category 2: 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	Customer energy usage 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 obtain attribute lists for targeted sales and marketing campaigns that may not be welcomed by those targets. Data may be used for insurance purposes.	Category 2: Under the existing metering and billing systems, meter data is not sufficiently granular in most cases to reveal any detail about activities. However, with 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 earlier in this chapter (see §5.3.1). Especially when collected and analyzed over a period of time, this information can provide a basis for determining occupant activities and lifestyle. For example, a forecast may be made about occupancy, sleep schedules, work schedules, and other personal routines.[73]

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

[73] *See* M.A. Lisovich, D.K. Mulligan, and S.B. Wicker, "Inferring Personal Information from Demand-Response Systems," *IEEE Security & Privacy* 8(1), January-February 2010, pp. 11-20, http://dx.doi.org/10.1109/MSP.2010.40 (presenting the results of an initial study in the types of information than can be inferred from granular energy consumption data); s*ee also* Footnote 65.

example, residential demand-response systems,[74] marketing,[75] and law enforcement.[76] 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 privacy concerns that may arise from potential uses of smart grid data. The table also lists a variety of parties that may 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 with access to customers' personal data 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 are aware of various potential uses of 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 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.

[74] Federal Energy Regulatory Commission, *2008 Assessment of Demand Response and Advanced Metering: Staff Report*, December 2008, http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf [accessed 8/11/2014] (discussing various types of demand-response systems and pricing schemes, including those for residential *customers).*

[75] E. Protalinkski, "Facebook, Opower, NRDC launch energy use app," *ZDNet*, April 3, 2012, http://www.zdnet.com/blog/facebook/facebook-opower-nrdc-launch-energy-use-app/11332 [accessed 8/11/2014].

[76] Law enforcement already uses energy consumption data to try to identify potentially criminal activity, like drug cultivation. *See e.g., United States v. Golden Valley Electric Association*, No. 11-35195, http://www.ca9.uscourts.gov/datastore/opinions/2012/08/07/11-35195.pdf [accessed 8/11/2014]. More granular data will provide law enforcement with more valuable information that may be able to identify a wider range of illegal activities.

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[77]	Specific Potential Uses of this Type of Data
Detailed energy usage at a location, whether in real-time or on a delayed basis.	*Personal Behavior Patterns and Activities Inside the Home*[78] 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, potentially what they are doing,	Utilities	Primary	Load monitoring and forecasting; demand response; efficiency analysis and monitoring, billing.
		Edge Services[79]		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).
		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.[80]

[77] "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.

[78] For more discussion on this, see §5.3.1.

[79] 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 apps built to utilize Green Button data, or consulting services based upon electricity usage.

[80] 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," FoxNews.com, February 28, 2007, http://www.foxnews.com/story/2007/02/28/gore-high-energy-use-home-target-critical-report/ [accessed 8/11/2014].

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[77]	Specific Potential Uses of this Type of Data
	and where they are located in the home.	Creditors		Determine behavior that seems to indicate creditworthiness or changes in credit risk.[81]
		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; corporate espionage—determine confidential processes or proprietary data.
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/Energy Service Provider	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.
Consumer-owned equipment and capabilities.	*Identify Household Appliances* Identifying information (such as a MAC address); directly reported usage information	Utilities	Primary	Load monitoring and forecasting; efficiency analysis and monitoring; reliability; demand response; distributed energy resource management; emergency response.

[81] 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.*, C. Duhigg, "What Does Your Credit-Card Company Know About You?" *New York Times Magazine*, May 12, 2009, http://www.nytimes.com/2009/05/17/magazine/17credit-t.html [accessed 8/11/2014].

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[77]	Specific Potential Uses of this Type of Data
	provided by "smart" appliances. Data revealed from HAN or 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.
		Appliance Manufacturers		Determine usage and/or condition of appliances, potentially in order to offer repair, replacement, and/or warranty services.
		Marketers		Profile for targeted advertisements based upon owned and un-owned 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; introduce a virus or other attack to collect personal information.

As seen in the table, 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, the press, 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; if associated with data that identifies an individual resident, either could indicate that the resident suffers from a particular disease or condition that requires the device.[82] 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.[83] Electricity usage data could also reveal how much the resident sleeps and whether he gets up in the middle of the night.[84] 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.[85] 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 that could be made with such data.

5.6.2 Wireless Access to Smart Meters and Secondary Devices

Future designs for some smart meters and many secondary devices (e.g., smart appliances and smaller devices) may incorporate wireless-enabled technology to collect and transmit energy usage information for homes or businesses.[86] 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.[87] There are well-known vulnerabilities related to wireless sensors and networks,[88] and breaches of wireless technology that may result in breaches of privacy.[89] For example, "war driving" is a popular technique used to locate, exploit, or attack insufficiently

---

[82] S. Lyon and J. Roche, "Smart Grid Privacy Tips Part 2: Anticipate the Unanticipated," *SmartGridNews.com*, February 9, 2010, http://www.SmartGridnews.com/artman/publish/Business_Policy_Regulation_News/Smart-Grid-Privacy-Tips-Part-2-Anticipate-the-Unanticipated-1873.html [accessed 8/11/2014]. To be clear, the data being discussed would be customer energy usage data that may be used to infer the presence of certain health-related equipment or appliances, and not specific health data. For a discussion about granularity of this data and what is possible to infer from it, see §5.3.1.

[83] 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 (E.L. Quinn, "Privacy and the New Energy Infrastructure," CEES Working Paper No. 09-001, Fall 2008, p. 31, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731 [accessed 8/11/2014]). He suggests that smart grid data could be used to see how often a treadmill was being used in the home.

[84] From Privacy by Design: Information and Privacy Commissioner of Ontario, and The Future of Privacy Forum, *SmartPrivacy For the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, November 2009, 27 pp., http://www.ipc.on.ca/images/Resources/pbd-smartpriv-Smart Grid.pdf [accessed 8/11/2014] (describing the types of information that could be gleaned from combining personal information with granular energy consumption data).

[85] Id. at page 11.

[86] Office of the National Coordinator for Smart Grid Interoperability, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*, NIST Special Publication 1108R2, National Institute of Standards and Technology, February 2012, p. 24, http://nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf [accessed 8/11/2014].

[87] *See* Table 5-2 Potential Privacy Concerns and Descriptions.

[88] *See, e.g.*, M.F. Foley, "Data Privacy and Security Issues for Advanced Metering Systems (Part 2)," *SmartGridNews.com*, July 1, 2008, http://www.smartgridnews.com/artman/publish/industry/Data_Privacy_and_Security_Issues_for_Advanced_Metering_Systems_Part_2.html [accessed 8/11/2014].

[89] Id.

protected or improperly configured wireless systems.[90] Readily available portable computing devices are used to detect signals emanating from wireless technology. If wireless technology is used to transmit energy consumption information for a unique location or dwelling, then that usage data should be protected from unauthorized use, modification, or theft, even if it is being transmitted for purposes of later aggregating to protect privacy.[91]

Since the utilities most frequently would not be receiving usage data from secondary devices, such as smart appliances, that data would not necessarily be protected in the same manner as usage data collected from a smart meter. For a discussion on recommended privacy protection practices for Third Parties not receiving the data from a utility, see §5.7.

5.6.3 Commissioning, Registration, and Enrollment for Smart Devices[92]

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 §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.

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;[93] and
- Determining how the registration information is used, where it is stored, and with whom it is shared.

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

---

[90] *See* M. Bierlein, "Policing the Wireless World: Access Liability in the Open Wi-Fi Era," *Ohio State Law Journal* 67(5), 2012, pp. 1123-1185, http://moritzlaw.osu.edu/students/groups/oslj/files/2012/04/67.5.bierlein.pdf [accessed 8/11/2014].

[91] For a discussion on how data aggregation was addressed in the healthcare industry, *see* "Standards for Privacy of Individually Identifiable Health Information; Final Rule," *67 FR 53181*, August 14, 2002, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt [accessed 8/11/2014]. 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* H. Li, H. Yu, B. Yang, and A. Liu, "Timing control for delay-constrained data aggregation in wireless sensor networks: Research Articles," *International Journal of Communication Systems – Energy-Efficient Network Protocols and Algorithms for Wireless Sensor Networks* 20(7), July 2007, pp. 875-887, http://dx.doi.org/10.1002/dac.849). 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.

[92] The first four paragraphs of this subsection are taken from OpenHAN v1.95: UCA International Users Group, *UCAIug Home Area Network System Requirements Specification*, Draft v1.95, May 21, 2010, http://www.smartgridug.net/sgsystems/openhan/Shared%20Documents/OpenHAN%202.0/UCAIug%20OpenHAN%20SRS%20-%20v1.95%20clean.doc [accessed 8/11/2014].

[93] 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.

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 instances, 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 information, sufficient privacy protections should be in place to minimize the potential for a privacy breach.

5.7. SMART GRID DATA ACCESS BY THIRD PARTIES

In September 2010, the CSWG Privacy subgroup began looking at the issue of Third Parties gaining access to customer energy usage data (CEUD) and any resulting privacy concerns. The primary purpose was to ascertain what gaps there might be in existing guidelines or standards for the obligations of Third Parties to protect privacy, and how they get and handle CEUD. Although the membership of the Third Party Recommended Practices Team was somewhat fluid throughout the process, it was generally composed of individuals representing utilities, state public utilities commissions, vendors, privacy advocacy organizations, and NIST.

5.7.1 Change in Group Charter

The charter of the group was to address a perceived gap in standards, regulations and best practices that might apply to how Third Parties receive and handle CEUD, and how they protect the privacy of the related customers. The focus was on consumer data, rather than commercial. Initially, the group reviewed the California Public Utilities Commission (CPUC) Rules on CEUD privacy[94], the NAESB REQ.22 Standard, *Third Party Access to Smart Meter-based*

[94] "Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company," Decision 11-07-056, issued July 29, 2011 ("CPUC Decision"), http://docs.cpuc.ca.gov/PublishedDocs/WORD_PDF/FINAL_DECISION/140369.PDF [accessed 8/11/2014].

Information Model Business Practices (MBPs) [95] (2011), and the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) Third Party Access Security Profile v1.0. From these three primary documents, a fourth document was put together as an all-encompassing set of recommended practices for Third Party CEUD usage. Due largely to the work accomplished by NAESB on REQ.22, which addresses data given to Third Parties by utilities, a more narrow focus for this group was later adopted. The initial work of the group clearly had overlap with the NAESB requirements, and so as to not give utilities potentially conflicting advice, this team sought to address only data Third Parties received from non-utility sources, such as in-home devices.

5.7.2 Additional Scope Determinations for Recommended Privacy Practices

While there may exist uncertainty over the extent to which any one government agency has regulatory oversight of Third Parties using CEUD, many agree that energy usage data (that will soon become more prevalent as the electric grid gains increased intelligence) can potentially be sensitive, privacy-impacting data in need of protection. This is particularly true when CEUD is combined with other data, such as an account number or smart meter IP address that then makes it identifiable to one premise or customer. The recommended privacy practices seek to provide suggestions as to how CEUD, and the data combined with it as just described, is best protected in order to protect personal privacy. The recommendations also may help educate consumers on what they should expect out of Third Parties with which they choose to share their data.

For purposes of these recommended practices, data provided to Third Parties by electric utilities or electricity providers was excluded. The distinction is also made between companies that are under contract to a utility or Third Party (Contracted Agents) and companies that do not have a contractual relationship with a utility (Third Party). Definitions from other sources were utilized where available.

In the present document, recommendations for how to protect privacy are made utilizing Fair Information Practice Principles (FIPPs). The basis for FIPPs is material found in the Privacy Act of 1974.[96] There are several versions of FIPPs commonly in use. The set used in this document includes Management and Accountability; Notice and Purpose; Choice and Consent; Collection and Scope; Use and Retention; Individual Access; Disclosure and Limiting Use; Security and Safeguards. When considering what recommendations might be made for Third Parties, the FIPPs provided the basic structure and baseline ideas for what should be done.

5.7.3 Recommended Privacy Practices

The full set of recommendations is found in Appendix D: Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties. The following provides a basic summary of the recommendations.

Privacy Notices

Third Parties should provide a privacy notice to customers prior to sharing CEUD with another party, or in the case of a significant change in organizational structure, such as merger, bankruptcy, or outsourcing, if it could impact the security or privacy of the data. Privacy policy

[95] Available for purchase at https://www.naesb.org/retail_standards.asp.

[96] 5 U.S.C §552a As Amended, http://www.justice.gov/opcl/privacy-act-1974 [accessed 8/11/2014].

notices should include information about how the Third Party will access, collect, use, store, disclose, retain, dispose of, and safeguard CEUD. The privacy notice should also detail how the customer may address complaints and/or revoke their authorization for the Third Party to have and use their CEUD.

Customer Authorization for Disclosures

Third parties should seek customer authorization prior to disclosing CEUD to other parties unless the service for which the data disclosure is necessary has been previously authorized by the customer. Customers should have access to their CEUD, and should be able to request corrections to the CEUD be made.

Data Disclosure and Minimization

In following with the FIPPs, a Third Party should not be collecting more than what is required to fulfill the agreed upon service, and a separate customer authorization should be obtained before CEUD is used in a materially different manner. There are, however, some exceptions that may be made. Aggregated data may be shared to provide an authorized service without disclosure to the customer. There may also be instances in which law enforcement seeks data via subpoena or court order, or perhaps situations in which there is a risk of imminent threat to life or property. In these instances, data may be disclosed without prior notice.

Customer Education & Awareness

Third Parties should educate customers about the Third Party's CEUD privacy protection policies and practices, including the steps the Third Party is taking to protect privacy. Customers should also be provided with a notice that the data they collect via in-home devices (or data from the meter that has not yet been validated) may differ from what the customer may receive on their bill from the Utility.

Data Quality

Data should be as accurate and complete as possible, recognizing that the data will be only as accurate and complete as the information received.

Data Security

Third parties should have clear data security policies that should be periodically reviewed and updated. They should have specific personnel to handle these policies and to ensure that their privacy practices are transparent to customers.

Privacy Practices Risk Assessment

Periodic assessments of the privacy practices should be performed. Assessments should also be considered in the case of a significant change in organizational structure that may impact privacy, when new privacy-related laws or regulations become effective, or when an event occurs that may impact privacy, such as unauthorized disclosure of data. The development of privacy use cases may prove a helpful tool, not just for the Third Party, but also for those within the smart grid community that may be able learn from the experiences of others.

Data Retention and Disposal

Third parties should have clear policies and practices on how long data will be retained, as well as when and how CEUD will be disposed of. This should be detailed in the privacy notice given to the customer.

Data Breaches

Third parties should be aware of and adhere to any laws or requirements with regard to data breaches. These rules may apply to Third Parties or to Contracted Agents.

Employee Training

Employees of Third Parties and their Contracted Agents should be trained on the security and privacy practices necessary to protect customer CEUD.

Audits

Finally, the recommended practices discuss the use of independent Third Party audits of security and privacy practices. These audits may be useful in helping to identify issues before they become legitimate problems.

5.8. INTRODUCTION TO PLUG-IN ELECTRIC VEHICLES COMMUNICATION ISSUES

5.8.1 Background – Vehicle Data Systems

In recent years, embedded computers have become an integral part of automotive systems. The modern vehicle includes an interconnected network of dozens of embedded microcomputers wired together by a Control Area Network (CAN) bus defined by an array of International Organization for Standardization (ISO) and Society of Automotive Engineers (SAE) standards. These microcomputers are dedicated to specific functions such as automatic braking, ignition systems, engine functions, lighting controls, fuel delivery, on-board diagnostics (OBD), and "black box" data recorders. More recently, vehicle on-board entertainment and Global Positioning Systems (GPS) navigation systems have also become part of the vehicle's on-board computer network. Until recently, this on-board network has not been connected to the world outside the vehicle, except for a single OBD connector for plugging into repair shop diagnostic equipment.[97] Vehicle "black box"-stored data has been subject to subpoena by courts in litigation related to a variety of situations involving insurance claims, accident investigations, or other matters.[98] Otherwise the data has historically remained under the control of the individual using the vehicle.

5.8.2 New Electric Vehicle Privacy and Security Risks

With the introduction of plug-in electric vehicles (PEVs), this situation is poised to change dramatically. PEVs need to plug into premises-based charging equipment, commonly referred to as Electric Vehicle Service Equipment (EVSE), and need to communicate such parameters as the vehicle's battery state-of-charge to the premises charger in order to properly manage charging

[97] An exception is the case of the GMC *OnStar*™ system installed in certain models, a cellular phone-based communication system for automatic crash response, navigation, roadside assistance and vehicle diagnostics.

[98] For more on this topic, see §5.3.2.2.

(and potentially, discharging back into the premises or into the electric grid). However, once such a data connection is established, there is currently no technical limitation on the amount or type of data that may be acquired from the vehicle's computers or "black boxes." In theory, depending on how the vehicle is equipped, it is possible to learn where the vehicle had traveled, how fast, where it stopped, for how long, how many were in the vehicle, what they listened to, etc.

PEVs change how society fuels their vehicles. With this change comes the promise of increased use of cleaner and renewable energy resources. This promise, coupled with limited traditional energy resources and societal changes, is pushing nations toward greater use of PEVs. PEVs provide for freedom of travel without the total reliance on motor fuel to keep them going, as is the case with traditional vehicles. Rather, PEVs harness electrical power and store it in the vehicle for future use. Instead of merely "filling up," these vehicles "plug-in" to the power of the electric grid allowing individuals to re-energize their vehicles at home, work, the mall—wherever people are able to find a charging station.

PEVs are also raising privacy concerns. The internal memory of a PEV may contain information about the vehicle user's name, address, VIN#, location, maintenance history, driving patterns, and more. Hundreds of these data items are available to be viewed by anyone with access to the PEV's internal memory. A number of potential privacy impacts put the vehicle users at risk if these data items are not appropriately safeguarded. For example, the vehicle's location history could pinpoint a location pattern for the vehicle, and thus may put the driver in greater danger of being tracked or harassed if, for one possible example, his or her estranged spouse has access to the vehicle's data. Maintenance history could share relevant information about the vehicle user's adherence to the maintenance schedule, which could be pertinent to the manufacturer's warranty responsibilities. Because of these types of issues and the impacts they potentially have on individual privacy, it is important to understand how PEVs affect privacy, and what steps are necessary to mitigate the privacy risks associated with owning and operating a PEV.

All PEVs will have the ability to have two-way communication with other systems. PEVs need to communicate with EVSE in order to communicate with a charging station. This communication is necessary for charging to occur safely. For instance, the charging station needs the current state of charge of the PEV in order to compute its charging schedule.

PEVs may also have a need to communicate with a system in order to resolve billing for a charging service. When charging at a "home" station, differential rates may be used for PEVs. When at a remote charging station, it will frequently be needed for billing. There are a number of ways this communication may occur depending on several factors. At the time of publication, there is no large PEV charging infrastructure in place, partially due to the difficulties associated with determining how billing for a charging service will be handled.

For instance, one scenario is that the local charging facility is responsible for collecting payment, and in turn, is also responsible for paying an energy distributor for the energy used. In this case, it is very likely that the PEV will only communicate with the local charging facility's system, and the bill will be resolved much like paying for gasoline at a local station.

However, another scenario being proposed within the industry is to have the bill for charging services at a remote facility be added to the PEV user's "home" utility bill. In this case, data

about the PEV, including some sort of identifying information, will need to travel through the local charging station's system to the "home" utility's systems. The data will cross many systems during this process. There likely will be multiple telecommunications companies involved in transmitting this data to the correct recipient. There may be some sort of intermediate clearinghouse used to help properly route the data. If not, the local facility would need to be able to handle routing the data to 1 of over 3300 utilities in the U.S. The data may cross geographical and legal boundaries that likely will have implications for how the data should be handled, and possibly stored. This model quickly becomes more complicated than merely paying for gasoline at the pump.

Yet another scenario being proposed is that PEV users would have an account with an electric vehicle service provider (EVSP). As there were fewer than ten EVSPs in the U.S. at the time of publication, the routing of data from a local charging station to a billing system would be much simpler than trying to route such data to a particular utility. However, the data would still need to cross multiple systems with possible legal boundary and other issues in order to reach the EVSP's billing system.

The latter two scenarios have more potential challenges for protecting PEV consumer privacy. An identifier could be used to bill the correct person, which is a primary source of privacy concerns. Every time data travels from one system to another, the risk of that data being compromised or inappropriately accessed increases.

An alternative to charging is electric grid support through PEV "parking lots" in which vehicles are not only charged, but discharged to provide temporary grid support in times of peak demand. When used in discharge mode, credit on the home electric bill is a possibility, requiring many of the same billing considerations as remote station charging.

PEVs are also capable of sending information via telematics directly to manufacturers or other entities, bypassing utilities and the electric grid completely. However, since this communication capability does not involve smart grid entities, this is not within the scope of this document.

5.8.3 Potential Privacy Issues and Risks -- Possible Information Elements

When considering potential privacy risks, there are certain specific types of information that are likely to be of particular concern. These include—

1. VIN# or other identifier – a type of personal information
2. Charging history/state of charge – identifies whereabouts and home charging station
3. Location history – identifies patterns in daily activities
4. Driving behavior history – identifies patterns in driving behavior
5. Maintenance history – identifies how often the PEV is serviced and how the vehicle user maintains the vehicle
6. Utility account(s) information – contains personal information, such as address
7. Point-of-service payment information – identifies financial information which may include credit card or bank account information; types of personal information

8. Other account information (i.e., parking garages, etc.) – identifies possible information regarding the PEV user
9. IP or MAC address (if applicable) – can be used to spoof IP address for hacking or identity theft
10. PEV purchase information/history – private or proprietary information, resale history

Any one of these pieces of information could pose a privacy risk by themselves. But when two or more of these elements are combined a greater potential privacy risk may exist. For example—

1. VIN# and charging locations/duration – May be used to track the travel times, locations, and patterns for the PEV user.
2. Name/identifier and PEV purchase information – Can notify potential thieves of location and type of vehicle, can enable inferences about income, can enable targeted advertising (e.g. charging facilities, etc.). Can also provide unfair competitive advantage to commercial entities when purchasing fleet vehicles.
3. Identifier, driving behavior history, and maintenance history – Can enable inferences for insurance and warranties, can enable targeted advertising for car-related services (e.g., mechanic services, high-risk insurance companies, etc.).
4. Utility account information and point-of-service payment information – can provide insight to personal information as well as account information, allowing the possibility of identity theft and/or credit card fraud.

5.8.4 Approaches to Mitigation of Risks

The new data privacy and security risks introduced with PEVs extends the discussion about smart meter data privacy into a larger dimension. Although the issue is potentially complex, two basic approaches can be used to help address the privacy risks, as in the case of other home appliances and networks:

1. Structurally contain the vehicle data within a home or premises network, and constrain access to it under the control of a premises gateway/firewall that enforces data privacy and security policies.
2. Establish legal, regulatory, and/or industry voluntary enforcement of privacy policies.

The first approach was identified in NISTIR 7628 (2010) Volume 2, pp. 37-38 with regard to consumer energy management systems (EMS). It is also the approach taken by recent regulatory initiatives in Germany and The Netherlands mandating an independent standardized gateway that controls and manages all access to all metering devices and other home energy applications and appliances (including PEVs) to ensure consumer data privacy and security.[99] For example, the

[99] Bundesamt für Sicherheit in der Informatioinstechnik [Federal Office for Information Security] (BSI), *Protection Profile for the Gateway of a Smart Metering System*, v1.3 (final release), March 31, 2014, http://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf [accessed 8/11/2014].

Privacy and Security Working Group, Netbeheer Nederland (NN), *Privacy and Security of the Advanced Metering Infrastructure*. Anahem, The Netherlands: NN, 2011. It may be worth noting that different countries have different market requirements and structures, such as state commission authorities, small municipal, or co-op structures, which may significantly limit the options when considering global implementations.

vehicle user could have the right and ability to erase, limit, or block data from being stored or transferred beyond the vehicle or premises such as is being done in the case of some computer browsers (e.g., *CCleaner* removes browsing history recorded by Firefox and Explorer browsers).

5.8.5 Looking Forward

Technical standards for premises systems and vehicle systems are currently under development that could support both privacy risk mitigation approaches. Currently regarding PEVs, there are essentially no technical safeguards to protect data stored in internal memory. Policy makers have the opportunity now to identify policies and to guide standards development in a way that could avoid future problems.

Specific solutions or mitigations for these potential privacy issues will need to be explored as technology solutions are deployed going forward. System and infrastructure architects and engineers should, in the meantime, stay aware of these potential issues. The Privacy Subgroup will endeavor to conduct more research in this area before the next revision of this document occurs.

5.9. AWARENESS AND TRAINING

Providing effective information security and privacy training and awareness not only supports privacy principles but also helps to ensure that workers, throughout all entities within the smart grid, have the knowledge necessary to keep personal information and energy usage data assets appropriately secured during their daily work activities. There is also a growing number of laws and regulations that include requirements for organizations to provide some type of information security and privacy training and awareness communications to not only their personnel, but also in some instances to their customers and consumers. Just a few examples of these include the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA) and the Gramm Leach Bliley Act (GLBA).

In addition to employee education, consumer education on privacy supports informed decisions related to participating in the deployment of smart grid technologies and granting access to the information such technologies enables. Concerns related to privacy can result in consumers opting out of smart meter deployment or in limiting access to customer energy usage data collected using smart grid technologies. All stakeholders have an important role in educating consumers on their rights as someone that will have their data collected to promote confidence in the way that such information is used and safeguarded from unauthorized use. To promote these objectives, information on privacy protections should be incorporated conspicuously into communications with consumers.

Likewise, raising awareness of privacy concerns for customer and energy usage data, and showing how those concerns are being addressed, may be an important aspect of managing relationships between various stakeholders. The audience for this training could include consumer advocates, legislators, state regulatory commissions, and utility companies.

It is important to note that while training and awareness are critical to overall understanding and acceptance of smart meter technologies, state PUCs/PSCs may not be the best avenue for seeking training. There are multiple areas where a PUC/PSC may lack in training abilities including resource and budget constraints, lack of jurisdiction, or political constraints stemming from public perceptions of their state utility commission. In general, state PUCs/PSCs where smart

grid functionalities exist may make an effort to educate customers using non-direct methods such as FAQ pages on their website, but should not be expected to roll out a public outreach campaign similar to the outreach programs created by utilities and/or Third Parties. PSCs/PUCs often mandate that utilities should create and execute well-defined public outreach campaigns that focus on educating customers about smart grid technologies as a part of their cost recovery stipulation. While not directly a product of state commissions, these campaigns are generally reviewed and approved by state commissions as being acceptable for public dissemination.

Through the efforts of several stakeholder categories, training slide sets have been developed by the CSWG Privacy Subgroup to assist various organizations with training employees, contracted workers, government entities, the private sector, and the general public on privacy implications and protections specific to the smart grid. These slide sets[100] include training materials for the following groups:

- Utilities
- State PUCs/PSCs
- Third Party Service Providers
- Consumer Advocacy Groups

These training and awareness slides may be used by organizations as a starting point for those within organizations planning information security and privacy education programs as they relate to smart grid privacy. These slides provide information as a way to help "train the trainer" -- providing advice and assistance for the organizations to create their own awareness and training content. There is significant additional information within the speaker notes, along with many pointers to other information resources, that organizations may wish to use when delivering their own tailored training.

The slide sets were created to assist organizations in developing their own training regimen and should not be considered as legal advice under any circumstances. Note that these slides are not endorsed by NIST, nor are they required to be used under any existing law or regulation.

5.10. 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 operationally necessary.

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, recipients of smart grid services 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

[100] See https://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy#Privacy_Training_Slides [accessed 8/11/2014].

(see Appendix F: Summary of the Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment).

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 certain areas of concern described in §5.6, Table 5-2.[101] However, because of the current technology used for the collection of the data, some concerns may need to be addressed by other means.

Many of the concerns relating to the 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. Such 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 include aggregated load control results for the entire household, rather than individual appliance data. 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 §5.3.1. 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 premises.

5.10.1 Existing Privacy Standards and Frameworks

The following represents a list of some existing standards and frameworks that can supplement the use cases documented here that applied the OECD Privacy Guidelines (see Appendix E).

1. *ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management: Section 15*. The International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC) jointly issued this international standard, last updated and published in December 2005. It is part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards. It is the Security Compliance Standard. ISO/IEC 27002 provides a security framework. Section 15 covers Compliance, including legal requirements; security policies and standards and technical compliance; and Information systems audit considerations. It is part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards.
2. *ISO/IEC 29100: Information technology — Security techniques — Privacy framework.* This international standard published in December 2011 provides a privacy framework which specifies a common privacy terminology; defines the actors and their roles in

[101] For a discussion regarding current legal and regulatory developments regarding energy usage data, see §5.3.

processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology.

3. *ISO/IEC 15944-8: Information technology — Business Operational View —Part 8: Identification of privacy protection requirements as external constraints on business transactions.* Modeling business transactions using scenarios and scenario components is done by specifying the applicable constraints on the data content using explicitly stated rules. External constraints apply to most business transactions. This part of ISO/IEC 15944 describes the business semantic descriptive techniques needed to support privacy protection requirements when modeling business transactions using the external constraints of jurisdictional domains. It was published in April 2012.

4. *Fair Information Practice Principles (FIPPs)*. The FIPPs are a set of principles that are rooted in the tenets of the Privacy Act of 1974. Several slightly different versions are used by various U.S. Federal Agencies, including the Department of Homeland Security (DHS), the Federal Trade Commission (FTC), and the Department of Commerce (DOC). For DHS, the FIPPs are Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. For the FTC, they are Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, and Enforcement/Redress.

5. *American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants (CICA) Generally Accepted Privacy Principles (GAPP) (a.k.a. AICPA/CICA GAPP).* These privacy tools include a universal framework for CPAs to conduct risk assessments and provide criteria to protect the privacy of personal information. The AICPA/CICA GAPP's Security for Privacy Principles has been mapped to ISO/IEC 27002. [102]

6. *European Union (EU) privacy framework.* The European Commission has proposed reforms to existing 1995 data protection rules that include a single set of rules on data protection that include a policy communication, a regulation setting out a general EU framework for data protection, and a directive to protect personal data processed for judicial activities.[103]

7. *APEC Privacy Framework.* Published in 2005, this framework establishes and promotes an approach to protecting privacy when sharing information throughout Asia-Pacific Economic Cooperation (APEC) member countries, with a goal of removing barriers to the free flow of information.[104]

8. *Privacy by Design (PbD).* This is a privacy framework by Ann Cavoukian, PhD, Information & Privacy Commissioner of Ontario. PbD promotes the proactive incorporation of privacy as the default and data protections embedded throughout the

[102] See http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx [accessed 8/11/2014].

[103] See http://ec.europa.eu/justice/data-protection/index_en.htm [accessed 8/11/2014].

[104] See more at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx [accessed 8/11/2014].

entire lifecycle of systems and technologies. The 7 Foundational Principles of PbD were published in August 2009 and revised in January 2011.[105]

9. *FTC Privacy Framework*. The Federal Trade Commission, America's chief privacy policy and enforcement agency, issued this final report setting forth best practices for businesses to protect the privacy of American consumers and give them greater control over the collection and use of their personal data. The final privacy report expands on a preliminary staff report the FTC issued in December 2010.[106]
10. *The Consumer Privacy Bill of Rights*. The Obama Administration released this document in February 2012, as part of a comprehensive blueprint to improve consumers' privacy protections and ensure that the Internet remains an engine for innovation and economic growth. The blueprint will guide efforts to give users more control over how their personal information is used on the Internet and to help businesses maintain consumer trust and grow in the rapidly changing digital environment.[107]
11. NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J, Privacy Control Catalog*. The purpose of this publication is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.[108]

5.10.2 Privacy Mitigation Tools and Activities

The mitigation of privacy risks is a process that seeks to minimize negative impacts to privacy. It encompasses a wide range of privacy management activities that identify threats and vulnerabilities to privacy for each business activity. Once a risk is identified, privacy mitigation processes attempt to match proportionate privacy controls for each relevant business activity that creates a risk to privacy. Described below are three widely used privacy mitigation processes: Privacy Impact Assessments, Privacy Audits, and Privacy Use Cases.

Privacy Impact Assessments.

A privacy impact assessment (PIA) is a structured process used to identify risks involved with—

- Fulfilling legal and regulatory obligations for managing, using, and sharing personal information.
- Collecting and using personal information only for the intended purposes.
- Ensuring the information is timely and accurate.

---

[105] See more at http://privacybydesign.ca/ [accessed 8/11/2014].

[106] "FTC Issues Final Commission Report on Protecting Consumer Privacy: Agency Calls on Companies to Adopt Best Privacy Practices," Federal Trade Commission [Press release], March 26, 2012, http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy [accessed 8/11/2014].

[107] "We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online," The White House [Press release], February 23, 2012, http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights [accessed 8/11/2014].

[108] See http://dx.doi.org/10.6028/NIST.SP.800-53r4.

- Ensuring the information is protected according to applicable laws and regulations while in the organization's possession.
- Determining the impact of the information systems on individual privacy.
- Ensuring individuals (e.g., employees, customers, etc.) are aware of the information the organization collects and how the information is used.

Any organization that collects personal information, or information that can reveal information about personal activities, can identify areas where privacy protections are necessary by performing a PIA. A PIA can be performed internal to the organization, or by an objective independent entity.

Audits.

An audit is a structured evaluation of a person, organization, system, process, enterprise, project or product. Audits can be used to determine compliance levels with legal requirements, identify areas where policies are not being followed, and so on. An audit should ideally be performed by an objective entity that is independent of the entity being audited.

Privacy Use Cases.

A Privacy Use Case is a method of looking at data flows that will help entities within the smart grid to rigorously track data flows and the privacy implications of collecting and using data. It is intended to help organizations address and mitigate the associated privacy risks within common technical design and business practices. Use cases can help smart grid architects and engineers build privacy protections into the smart grid. Privacy protection designed into a system is preferable to a privacy patch or "work around" in an attempt to remedy a limitation or omission.

The Privacy Use Cases presented in Appendix E of this document are focused on data privacy in selected smart grid scenarios[109], making them unique amongst the many tools, frameworks, and standards that are noted above. These Privacy Use Cases reflect the electricity value chain and the impacts that smart grid technologies, new policies, new markets, and new consumer interactions will have on the privacy of personal data. The Privacy Use Cases can serve as a valuable tool for all types of smart grid entities to better understand the implications of smart grid changes to existing processes and procedures. These smart grid entities include utilities; energy service companies (ESCOs); vendors of products and services that may include collection, storage, or communication of personal data; and policy-makers.

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 which privacy concerns 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

[109] The key Use Cases deemed architecturally significant with respect to security requirements for the smart grid in NISTIR 7628 (August 2010). The CSWG Privacy Subgroup took those use cases verbatim and added the privacy considerations for each associated use case.

those responsible for creating, implementing, and managing the controls that impact privacy to do so more effectively and consistently.

5.10.3 Privacy Use Case Scenarios

The Privacy Subgroup spent many months creating a few different methods for expanding the existing NIST collection of use cases[110] to include consideration of privacy concerns. When considering which set of FIPPS to use for creating privacy use cases, it was decided to use the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines. They are—

- Long-established and widely recognized;
- Freely available; and
- Straightforward concepts that will be more easily and consistently utilized when building privacy controls into processes.

The larger set of principles used to conduct the smart grid PIA was 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 E contains the full set of privacy use cases.

5.11. EMERGING SMART GRID PRIVACY RISKS

Seamless and rapid access to energy usage data can benefit consumers by helping them to manage costs and to conserve energy but may also introduce additional privacy risks. In addition to addressing the other current risks identified within this report as a whole, organizations and consumers utilizing smart grid systems, applications, and related technologies should also be aware that new threats to privacy, and vulnerabilities within new technologies and practices, will continue to emerge over time and as capabilities and technologies evolve. Interconnected networks (e.g., smart phones that utilize cloud services) expand the opportunities for privacy data breaches. While such risks are not unique to the smart grid, they may introduce new types of issues that will need to be addressed as the smart grid evolves. Some of the new and emerging technologies and activities that were not yet widely deployed or in existence within the smart grid at the time of this report, but that are being discussed and could introduce different privacy challenges, include:

[110] See the collection of use cases that the Privacy Subgroup considered and chose as representative use cases: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases [accessed 8/11/2014].

1. **Customer energy usage data (CEUD) and personal consumer data being sent to smart phones and other mobile computing devices**. Sending data from centrally controlled and secured systems to such devices as smart phones and mobile computers puts that data under the control of the associated users. While such information can be very useful to those users, if the data is not appropriately secured, the data can be breached. This type of decentralization of sensitive and personal data has led to significant privacy breaches through mobile computing devices[111]. Additionally, CEUD and personal consumer data stored on mobile computing devices are difficult to track and maintain.

2. **CEUD and personal consumer data being sent to social media sites, or social media sites being used to control end devices**.[112] In recent years, data that used to be stored only on secured business servers have been put onto social media sites, resulting in unauthorized disclosure and the loss of trust in the organizations responsible for the data. Often workers with authorized access to the sensitive data have been careless, or lacked appropriate privacy and security training.[113]

3. **CEUD and personal consumer data being stored, managed, or otherwise accessed from cloud services**. Sensitive data stored and managed by cloud services have been breached on numerous occasions. In a recent study, over half of the organizations surveyed are not currently using cloud services because of the related security concerns.[114] Organizations within the smart grid should be aware of the risks related to the use of cloud services if or when they consider moving some smart grid activities to such cloud services.

4. **The creation of new applications (apps) that collect CEUD and personal consumer data**. According to a recent study, most workers now are spending a significant amount of time each day using apps on mobile devices and are expected to spend more time doing so than browsing the Internet on those devices.[115] There is a growing number of apps, and the

---

[111] As reported in the Pew Research Center report, *Privacy and Data Management on Mobile Devices* (September 5, 2012), "smartphone owners are also twice as likely as other cell owners to have experienced someone accessing their phone in a way that made them feel like their privacy had been invaded. Owners of smartphones and more basic phones are equally likely to say their phone has been lost or stolen." See http://pewinternet.org/~/media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf, p. 3 [accessed 8/11/2014].

[112] S. Soundation, *4 Channel Arduino-based Twitter control for home appliances!*, January 11, 2012. http://www.youtube.com/watch?v=n3S5CDm7IPk [accessed 8/11/2014].

[113] According to a Ponemon Institute survey report, *The Human Factor in Data Protection* (January 2012), employees are the root cause of many data breaches due to their negligence or malicious behavior, and 78 % of the survey respondents indicate that employee behaviors, both intentional and accidental, were cited as leading to at least one data breach within their organizations over the past two years. One of the primary reasons listed was the "use of social media in the workplace." See http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-executive-summary.pdf [accessed 8/11/2014].

[114] According to a global cloud survey conducted by Trend Micro in August, 2012, more than half (53 %) of decision makers surveyed said that data security was a key factor in their decision to "put the brakes on" cloud adoption. See S. Hoffman, "Study: Data Security Biggest Cloud Inhibitor," *ChannelNomics.com*, August 30, 2012, http://channelnomics.com/2012/08/30/study-security-biggest-cloud-inhibitor/ [accessed 8/11/2014].

[115] According to a September 12, 2012 Flurry Analytics report, mobile phone users spend over 1.5 hours a day on average on applications, and the number continues to grow. The time spent by users on apps is now beginning to surpass the time spent on the Internet on mobile devices. See P. Depuy, "Surfing your smartphone: who's watching you?" *Prime Social Marketing*, September 12, 2012, http://www.primesocialmarketing.com/surfing-your-smartphone-whos-watching-you.html#.U_YMoWOFlHo [accessed 8/11/2014].

quality of the security built into these apps varies widely. A growing number post information to online sites without the app users' knowledge.[116]

5. **Smart meter reading capabilities for individual premises so that a home area network (HAN) or other device may monitor in smaller intervals, as well as in real-time**. As discussed in other areas of this report, the more frequently energy usage readings occur, the more detailed information can be inferred about the related personal activities. As customers consider installing advanced technology, all parties involved should consider the potential privacy impacts of using that technology or service.

6. **Including CEUD and energy consumer data in "Big Data"[117] files and their associated analysis activities**. Seemingly benign data can have consequences when amassed, analyzed, cross-referenced, and correlated with other databases. Analyzing energy usage data and/or consumer personal data may reveal information about the associated individuals' activities, habits, and lifestyles. When this data is combined with other data in Big Data repositories, it may enable useful and needed energy management breakthroughs that benefit both the individual and society by using powerful Big Data analytics. However, the activities may also reveal personal information about individuals that, until the advent of Big Data and associated analytics, had not yet been able to be accomplished.[118] If smart grid entities consider the use of Big Data, they should also consider the associated new ways in which Big Data analytics can reveal consumer information and energy consumption activities. In addition, regulators and other legal authorities may wish to consider Big Data analytics and possible consequences.

7. **Connecting smart appliances and HANs directly to the smart grid**. Utilities are already seeing the benefits of consumers using their HANs to help self-manage their energy use, as well as improving the ability for utilities to manage service to customers.[119] If smart grid entities continue along this path, they should also consider the associated privacy risks that will accompany connections of consumer HANs to smart meters or other smart grid components.

8. **Green Button developments that bring privacy risks**. Utilities are working with software companies to enable energy customers to transfer their own energy data to authorized Third Parties using new Green Button energy application program interfaces (APIs) and data sets. The Green Button initiative is resulting in innovations, and possibly new types of

---

[116] Secure.me analyzed approximately 500,000 Facebook apps and found 63 % of those apps ask for the ability to post on the app user's behalf. See C. Taylor, "Most Facebook Apps Can Post Behind Your Back [updated]," *Mashable*, September 4, 2012, http://mashable.com/2012/09/04/most-facebook-apps-post-behind-your-back-exclusive/ [accessed 8/11/2014].

[117] The term "Big Data" refers to digital data volume, velocity and/or variety that can enable novel approaches to frontier questions previously inaccessible or impractical using current or conventional methods; and/or exceed the capacity or capability of legacy or conventional methods and systems.

[118] In Microsoft's *Trustworthy Computing Next* report, an entire section is devoted to discussing privacy issues related to Big Data that are similar to this. See S. Charney, *Trustworthy Computing Next*, version 1.01, Microsoft Corporation, February 28, 2012, http://blogs.technet.com/b/security/archive/2012/08/27/computing-trends-cloud-big-data-and-the-evolving-threat-landscape.aspx [accessed 8/11/2014].

[119] L. Margonelli, "Could the Smart Grid Finally Do Some Good for Consumers?" *Pacific Standard*, September 26, 2012, http://www.psmag.com/environment/could-the-smart-grid-finally-do-some-good-for-consumers-46882/ [accessed 8/11/2014].

technologies, to provide energy data transfer paths to authorized Third Parties.[120] The vendors creating these new Green Button technology solutions should build in controls to address any new types of privacy risks that emerge with the new technology solutions.

9. **Linking or tracking (e.g., GPS) consumer activities and movements with energy usage data**. Law enforcement and investigators have been tracking vehicle activities through the use of GPS for several years to help with cases and solving crimes. There are now GPS devices that track fuel use as it relates to driving behavior.[121] If these types of monitoring tools are expanded to tracking PEVs, and then connected to other networks that are part of the smart grid, the related privacy issues need to be addressed. Likewise, if any other types of mobile energy-using appliances or other devices are connected to a HAN or other smart grid components, the impact of combining the GPS and related locational data with the energy usage data should be assessed for new privacy risks.

10. **Sharing smart grid data across national borders**. Energy usage data, focused at the transmission and distribution level, but not individual consumer, is currently shared from the U.S. to Canada. Energy data is also currently shared across borders throughout the European Union (EU),[122] as well as other locations throughout the world. If the U.S. plans to share more types of data that would involve individual consumer data, created through any of the smart grid components with another country, then the privacy impacts of such new types of cross border data flows should be evaluated.

11. **Wireless smart grid data transmissions, including near field communications (NFC) as well as wide area wireless communications**. Smart meters and associated devices may collect energy usage data from inside the home, store it, and send it to the utilities through wireless Internet or other connections. If plans emerge to start transmitting energy usage and/or customer data from HANs into smart meters, or other types of existing or future smart grid components, then those wireless transmissions will bring privacy risks, and controls should be established to protect the transmissions from inappropriate use.

12. **Linking biometrics with the smart grid**. Biometrics are currently used to accomplish strong authentication for secured networks and systems. Biometric encryption is currently being used within Canada to secure smart meter and other smart grid transmissions.[123] Biometrics provide a strong way to perform authentication and encryption. However, the biometric identifier itself provides information about an individual that needs to be strongly controlled and secured. If utilities and smart grid vendors start exploring biometric

---

[120] See "3 promising developments on the road to energy empowerment," *SmartGridNews.com*, October 2, 2012, http://www.smartgridnews.com/artman/publish/Business_Consumer_Engagement/3-promising-developments-on-the-road-to-energy-empowerment-5162.html/#.UHsRZMXA9V4 [accessed 8/11/2014].

[121] See A. Chang, "Tracking Behavior Behind the Wheel," *Forbes.com*, September 27, 2012, http://www.forbes.com/sites/altheachang/2012/09/27/tracking-behavior-behind-the-wheel/ [accessed 8/11/2014].

[122] See "Smart grids: Making connections," EurActiv.com, December 22, 2011, http://www.euractiv.com/energy/smart-grids-making-connections-linksdossier-509908 [accessed 8/11/2014].

[123] See K. Anderson, "Practical Privacy by Design: Examples of Success," [Presentation], June 13, 2012, http://www.pcpd.org.hk/pbdconference/files/Anderson_Part2.pdf [accessed 8/11/2014].

authentication and/or encryption methods for use within the smart grid, then they should determine how to acceptably secure those biometric data files.

13. **New types of malware within the smart grid**. There are ever increasing types of malware throughout all systems and networks. Many types of mobile malware exist whose sole purpose is to steal data from mobile devices, with the goal of obtaining as much personal data as possible.[124] Many of these privacy-stealing malware are delivered through apps, while others are delivered through online sites. It is a growing occurrence for personal data stealing malware to be represented as anti-malware tools.[125] As new apps, tools, and technologies emerge for smart grid components, organizations should be vigilant for new types of malware created to steal data collected through various smart grid technologies such as smart meters and smart appliances.

14. **New risks created by adding other utilities (e.g., water, gas, etc.) into the smart grid.** Many utilities also currently provide water and/or gas services. Usage data from those services may provide additional insights into personal activities, possibly creating additional privacy risks. If water and gas data are combined with electricity usage data within the smart grid, more information about lifestyles and individual activities may be revealed. Additional research should be used to identify any additional privacy risks accompanying the incorporation of water and gas usage within the smart grid.

15. **Ensuring "intelligent" systems that react to smart grid activities do not invade privacy as an after-effect**. Intelligent software that has the ability to control and make changes to different components within the smart grid, based upon systems settings, patterns, and other factors, can provide great benefit to managing energy usage. However, as has already been demonstrated,[126] if the intelligent systems are compromised, such as through the supporting code or through access to the systems themselves, potentially immeasurable amounts of damage could occur. Some of this damage could include access to customer and/or energy usage data, and making data and energy usage alterations that impact dwelling environments and the individuals within them. As intelligent systems are created for use within the smart grid, attention should be given to how the planned systems can impact privacy.

All utilities and smart grid vendors that are planning to pursue any of these activities and technologies should keep privacy in mind, and address the associated privacy risks as they develop such services and solutions. Consumers considering making use of these advanced technologies and services should also be aware of the potential privacy trade-offs of using those technologies or services.

---

[124] See more information in L. Seltzer, "Mobile Malware Exists to Steal Your Data," *InformationWeek Government*, March 6, 2012, http://www.informationweek.com/byte/personal-tech/mobile-applications/mobile-malware-exists-to-steal-your-data/232602097 [accessed 8/11/2014].

[125] See more information in the thread "Removal Instructions for Privacy Protection," *Malwarebytes.org*, started November 6, 2011, http://forums.malwarebytes.org/index.php?showtopic=99247 [accessed 8/11/2014].

[126] See more information in "Cyber Security Risk to Smart Grids and Intelligent Buildings," *ScienceDaily.com*, August 13, 2012, http://www.sciencedaily.com/releases/2012/08/120813115448.htm [accessed 8/11/2014].

5.12. SMART GRID PRIVACY SUMMARY AND RECOMMENDATIONS

Based upon the work and research conducted since June 2009, and since the publication of the first version of NISTIR 7628 Volume 2 (August 2010), the Privacy Subgroup identified significant new privacy issues to address, created a number of tools for smart grid entities to use, and made a number of recommendations to mitigate privacy risks.

Creating a smart grid privacy principles program that individuals are willing to use continues to be a challenge. The goal is to have individuals participate in the smart grid, allowing the electric sector to thrive and innovation to occur. An indicator of success is the degree to which 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 volume for all entities that participate within the smart grid. The following provides a summary listing of all the recommendations from within this volume that can be used for quick reference by organizations to assist with their privacy mitigation efforts. This list provides only a brief description of each recommendation. For more details refer to the associated section as indicated below—

Sections 5.1 - 5.3

- No recommendations within these sections.

Section 5.4 and Appendix F Consumer-to-Utility Privacy Impact Assessment

1. **Management and Accountability**.

    - **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.
    - **Establish privacy audits.** Audit functions should be modified to monitor all privacy-related energy data access.
    - **Establish or amend incident response and 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**.

    - **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, in a clearly worded description of the data being collected, why it is necessary to collect the data, and the intended use, retention, and sharing of the data.
    - **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.

3. **Choice and Consent**.

- **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**.

- **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 customer.**

5. **Use and Retention**.

- **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.
- **Limit information retention.** Data collection that exceeds the purposes for which the data were originally collected can have financial consequences. For example, the existence and contents of databases about customers may be subject to civil and criminal discovery. Service providers may be obligated to hire staff to cull these databases in order to fulfill court orders. 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. After the appropriate retention period, data should be aggregated or destroyed.

6. Individual Access.

- **Access to energy usage data.** 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.

- **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.

- **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.
- **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.
- **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.

9. Accuracy and Quality.

- **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.

- **Policy challenge procedures.** Organizations collecting energy data, and all other entities throughout the smart grid, should establish procedures that allow 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 appropriate 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.
- **Establish breach notice practices.** Any organization with smart grid data should establish policies and procedures to identify breaches and misuse of smart srid data, along with expanding or establishing procedures and plans for notifying the affected individuals in a timely manner with appropriate details about the breach.

Section 5.5 Personal Information in the Smart Grid

All organizations participating in the smart grid should determine which data items will significantly lessen or remove the ability to link to specific addresses or individuals whenever they perform their data anonymization activities.

Section 5.6 In-depth Look at Smart Grid Privacy Concerns

5.6.7 Wireless Access to Smart Meters and Secondary Devices

If future wireless technology is used to transmit aggregate home or business energy consumption information for a unique location or dwelling, then that usage data should also be protected from unauthorized use, modification, or theft prior to sufficient aggregation to protect privacy.

5.6.8 Commissioning, Registration, and Enrollment for Smart Devices

- Privacy issues that should be addressed related to the registration of these devices with Third Parties include: determining the types of information that are involved with these registration situations; controlling the connections which transmit the data to the Third Party, such as wireless transmissions from home area networks; and determining how the registration information is used, where it is stored, and with whom it is shared.
- At each step in this process, the consumer, utility, and Third Party provider should 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.

Section 5.7 and Appendix D Smart Grid Data Access by Third Parties

For the full set of recommendations, see Appendix D. A concise overview of the recommendations is contained below.

- **Privacy Notices.** Third Parties should provide a privacy notice to customers prior to sharing customer energy usage data (CEUD) with another party, or in the case of a significant change in organizational structure, such as a merger, bankruptcy, or outsourcing.
- **Customer Authorization for Disclosures.** Third Parties should seek customer authorization prior to disclosing CEUD to other parties unless the service for which the data disclosure is necessary has been previously authorized by the customer.
- **Data Disclosure.** A Third Party should not be collecting more than what is required to fulfill the agreed upon service, and a separate authorization should be obtained before CEUD is used in a different manner.
- **Customer Education & Awareness.** Third Parties should educate customers about the Third Party's CEUD privacy protection policies and practices, including the steps the Third Party is taking to protect privacy.
- **Data Minimization.** In following with the FIPPs, Third Parties should collect only the CEUD they need to provide the service they offer and have an authorization for.

- **Data Quality.** Data should as accurate and complete as possible.
- **Data Security.** Third Parties should have clear data security policies that should be periodically reviewed and updated.
- **Privacy Practices Risk Assessment.** Periodic assessments of the privacy practices should be performed.
- **Data Retention and Disposal.** Third Parties should have clear policies on how long data will be retained, as well as when and how CEUD will be disposed of.
- **Data Breaches.** Third Parties should be aware of any laws or requirements with regard to data breaches. These rules may apply, not just to the Third Party, but also to their Contracted Agents.
- **Employee Training.** Employees of Third Parties and their Contracted Agents should be trained on the security and privacy practices necessary to protect customer CEUD.
- **Audits.** The recommended practices discuss the use of independent Third Party audits of security and privacy practices. These audits may be useful in helping to identify issues before they become legitimate problems.

Section 5.8 Plug-in Electric Vehicles Privacy Concerns

Specific solutions or mitigations for PEV potential privacy issues should be explored as technology solutions are deployed going forward. System and infrastructure architects and engineers should stay aware of potential issues.

Section 5.9 Awareness and Training

Organizations involved within the smart grid should provide privacy and information security training, supported by ongoing awareness communications, to their workers that have job responsibilities involving customer and energy usage data. Organizations should also consider providing information to their customers and the public to help them to better understand the privacy issues related to the smart grid, along with how the organization is working to mitigate the associated risks, and also steps the public can take to better protect their own privacy. Utilities, State PUCs/PSCs, Third Party providers, and consumer advocacy groups should consider using these as a starting point to help them effectively and efficiently plan for privacy education programs as they may relate to smart grid privacy.

Section 5.10 Mitigating Privacy Concerns within the Smart Grid

- **Perform privacy impact assessments (PIAs).** Any organization that collects personal information, or information that can reveal information about personal activities, can identify areas where privacy protections are necessary by performing a PIA. A PIA can be performed internal to the organization, or by an objective outside entity.
- **Perform Audits.** An audit is a structured evaluation of a person, organization, system, process, enterprise, project or product. Audits can be used to determine compliance levels with legal requirements, to identify areas where policies are not being followed, and so on. An audit should ideally be performed by an objective entity that is not a member of the area being audited.

- **Utilize the Privacy Use Cases.** Use cases can help smart grid architects and engineers build privacy protections into the smart grid. The Privacy Use Cases in this document are focused on data privacy in selected smart grid scenarios, making them unique amongst the many tools, frameworks, and standards that are noted above.

Section 5.11 Emerging Smart Grid Privacy Risks

- Entities should remain aware of emerging smart grid privacy risks.

Given these realities, findings, and recommendations, the Privacy Subgroup hopes that the information contained in this volume will serve as a useful guide and reference for the wide variety of smart grid stakeholders, policymakers, and lawmakers who have, or may have in the future, responsibility for consumers' personal information, including energy consumption data.

5.13. NIST PRIVACY-RELATED WORK

5.13.1 National Strategy for Trustworthy Identities in Cyberspace Concerns

In April 2011, President Barack Obama issued the National Strategy for Trusted Identities in Cyberspace[127] (NSTIC). NSTIC calls for the development of interoperable technology standards and policies — an "Identity Ecosystem" — where individuals, organizations, and underlying infrastructure can be authoritatively authenticated in cyberspace. The goals of the NSTIC include protecting against cyber crimes (i.e. identity theft, fraud), while simultaneously helping to ensure that the Internet continues to support the innovation of products and ideas.[128]

The Identity Ecosystem promotes the secure validation of identities when performing sensitive transactions (such as obtaining financial, health or energy usage data) while simultaneously allowing for anonymity in other situations (such as casually surfing the Web). The Identity Ecosystem could protect individual privacy by reducing the need to share personally identifiable information (PII) at multiple web sites and by establishing policies about how organizations use and manage PII in the Identity Ecosystem.[129]

Additional benefits of the Identity Ecosystem may include:

- **Speed**: One user and one key credential would authorize any password-protected website the user delegates. This feature is very similar to the existing banking structure that allows a client to use their PIN for ATM transactions here and abroad.
- **Convenience**: Individuals, business, and government agencies could perform secured and sensitive transactions online that now are conducted in person.

[127] "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy," *The White House*, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf [accessed 8/11/2014].

[128] "About NSTIC," [Web page], http://www.nist.gov/nstic/about-nstic.html [accessed 8/11/2014].

[129] *Ibid.*

- **Privacy**: Credentials would be intended to share only the amount of personal information necessary for the transaction, but allows for a choice of when to use or not to use a trusted ID.[130]

While the key framework of NSTIC calls for development by the private sector, the Department of Commerce established a National Program Office (NPO) to coordinate related federal activities that will advance the project's objectives.

As of May 2014, the NPO has taken two major steps forward. First, it contracted with a private organization to jump-start the public-private collaboration in August 2012. The Identity Ecosystem Steering Group has since established itself as a non-profit corporation and has held eight publicly open plenary sessions. It is in the process of developing the Identity Ecosystem Framework necessary to meet the NSTIC's goals. Second, the NPO has awarded twelve pilot projects that are intended to test or demonstrate new solutions, models or frameworks, motivated by the recognition that market forces alone have not been able to overcome various barriers to innovation. Such barriers include, but are not limited to:

- A lack of commonly accepted technical standards to ensure interoperability among different authentication solutions.
- Complex economic issues, including a lack of clarity related to liability (i.e., "who is liable if something goes wrong in a transaction?" "How – if at all – should transactions be monetized?").
- No common standards for privacy protections and data re-use.
- Challenges with usability of some strong authentication technologies.[131]

To help overcome some of these barriers, the Identity Ecosystem Framework promotes developing "policies for verifying identity and identity credentials; procedures for how identity credentials are used and verified through online authentication transactions; standards and technical specifications for conveying and securing identity information online, and; accountability measures to ensure all participants operate in accordance with defined rules."[132] The NSTIC NPO is currently reviewing applications for a third round of pilot projects to be awarded in the fall of 2014.

There are those that question the need for government action. A common criticism is that NSTIC will lead to an online national (or even worldwide) identity system that could discourage constitutionally protected speech and association, (such as anonymous speech). In addition, the Identity Ecosystem could create additional security and privacy concerns. For example, the Identity Ecosystem strategy could be compared to "creating a single skeleton key that, if cracked, could allow for a much greater security issue than a single site password breach."[133] Related

---

[130] "National Strategy for Trusted Identities in Cyberspace," [Web page], http://www.nist.gov/nstic/ [accessed 8/11/2014].

[131] "Announcement of Federal Funding Opportunity (FFO), National Strategy for Trusted Identities in Cyberspace (NSTIC) Pilot Grant Program," February 1, 2012, p. 5, http://www.nist.gov/nstic/2012-nstic-ffo-01.pdf [accessed 8/11/2014].

[132] Identity Ecosystem Steering Group (IESG), "The Proposed Identity Ecosystem Steering Group Workplan Outline," [August 3, 2012], p. 1, http://www.nist.gov/nstic/reports/IESG_Workplan_Outline.pdf [accessed 8/11/2014].

[133] K. Hickey, "Trusted Identities: Single sign-on or single point of failure?" *GCN*, February 1, 2011, http://gcn.com/articles/2011/02/01/trusted-identities-single-point-of-failure.aspx?m=2. [accessed 8/11/2014].

thereto, even though the process is entirely voluntary for the user, the increased acceptance of and preference for credentials by commercial websites could pressure even reluctant consumers to obtain NSTIC credentials, thereby greatly expanding the risks associated with such credentials.

Another chief privacy concern regarding the use of a single NSTIC credential to access multiple sites is that such credentials could be used to identify and track each unique user's online activity. Finally, credential issuing authorities could obtain leverage over website owners and consumers through not only their power to issue, but also potentially their ability to revoke credentials as well. There also is concern that since the system is being introduced by the government "individuals may be lulled into a false sense of security, believing it has appropriate safeguards in place to prevent security and privacy issues."[134]

The NSTIC NPO has addressed these concerns by developing a governance structure under a "multi-stakeholder" process that engages companies, government and consumer advocacy organizations on equal levels, and that currently has active participation and leadership from a number of privacy and consumer advocates. Under the Identity Ecosystem, relying parties would be dependent on identity providers, those that issue credentials, to validate the identity of users visiting the relying party's site. Accordingly, logic and history indicate that it may be difficult to initially recruit significant numbers of relying parties.[135]

To the extent NSTIC is implemented, the possibilities for incorporating the Identity Ecosystem into smart grid systems could be significant. For example, the NSTIC framework has the potential to affect utilities in multiple areas. In operations, NSTIC could allow field staff trusted access to company equipment using pre-authorized credentials without the need for additional verification from the management office. From the consumer's perspective, a user may have the ability to pay their utility bill without revealing credit card information simply by using the same credentials authorized by their financial institution, as well as have more secure access to Green Button[136] information. However, there are also likely to exist both additional positive and negative utility impacts that will not be known unless the NSTIC Identity Ecosystem comes to fruition.

In sum, the NSTIC Identity Ecosystem could change the paradigm for how energy usage information is accessed and shared, as well as if and when PII would be used or retained for identification purposes.

5.13.2 Privacy Engineering

NIST has begun a Privacy Engineering initiative that seeks to establish an outcome-oriented design framework for enhancing privacy within information systems. Process-oriented principles such as the Fair Information Practice Principles are an important component of an overall privacy framework, but on their own they do not achieve consistent and measurable results in privacy protection. In the security field, risk management models, along with technical standards

---

[134] *Ibid.*

[135] J. Fontana, "On 1-year anniversary, organized NSTIC looking for fast track," *ZDNet*, April 18, 2012, http://www.zdnet.com/blog/identity/on-1-year-anniversary-organized-nstic-looking-for-fast-track/424 [accessed 8/11/2014].

[136] Green Button is an industry-led effort that responds to a White House call-to-action: provide electricity customers with easy access to their energy usage data in a consumer-friendly and computer-friendly format. For more information, refer to: http://greenbuttondata.org [accessed 8/11/2014].

and best practices, are key components of improving security. Similarly, the safety risk management field also has well-developed models, technical standards and best practices. To date, the privacy field has lagged behind in the development of analogous components.

NIST's objective is to provide system owners, developers, and engineers with reusable, standards-based tools and privacy engineering practices that can be used to mitigate the risk of privacy harm in a measurable way within an organization's overall risk management process. The Smart Grid, like many other complex efforts, requires coordination across a wide range of disciplines – from engineers and system designers to legal and policy professionals. The Privacy Engineering initiative is intended to improve the ability of interdisciplinary teams to implement effective privacy practices, in part, by providing a common language that can be used across organizations.

NIST will engage a broad community of stakeholders to facilitate this work. To capture the findings from this outreach, NIST will produce a report that identifies challenges in privacy engineering, and proposes a framework for understanding privacy risk and a methodology for designing privacy-enabled systems that would support outcome-driven privacy design and engineering practices. NIST will hold workshops and formal public comment periods to maximize input from interested stakeholders. As the development of reusable tools and privacy engineering practices evolves, NIST may produce additional supporting materials.

APPENDIX C: CHANGING REGULATORY FRAMEWORKS

Beginning in 2010, the public utility commissions of California and Colorado conducted rulemaking proceedings to address privacy issues for customer energy usage data. Both proceedings involved collaborative processes and broad stakeholder involvement.

On September 29, 2010, California passed SB 1476 (California Public Utilities Code Secs. 8380 and 8381), which outlined privacy protections for electricity and natural gas usage data. Cal. P.U. Code Secs. 8380 and 8381 provide privacy protections for data generated by electrical and natural gas advanced meters used by both investor-owned and publicly owned utilities. Utilities cannot share, disclose or make available to a Third Party a customer's electricity or gas usage data generated by an advanced metering infrastructure without the consent of the customer, with limited exceptions. Those exceptions are when the data is used "for system, grid or operational needs, or [in] the implementation of demand response, energy management, or energy efficiency programs," or "as required or permitted under state or federal law or by an order of the" California Public Utilities Commission (CPUC). (California Public Utilities Code Section 8380(e)(2) and (3).) All other purposes, deemed "secondary purposes," require the consent of the customer. In addition, SB 1476 requires utilities to use "reasonable security procedures and practices" to protect a customer's unencrypted electric and gas usage data from unauthorized access, use or disclosure. SB 1476 also prohibits utilities from selling a customer's electric or gas usage data or any other personally identifiable information for any purpose.

SB 1476 was an update of and supplement to existing privacy statutes, regulations and tariffs dating from the early 1990s and already applicable to customer data held by utilities, such as Public Utilities Code Sections 394.4 (privacy protection for customer usage data obtained by non-utility electric service providers from utilities) and 2894 (privacy protections for customer information collected by telecommunications providers), and CPUC Decision No. 90-12-121, 39 CPUC 2d 173 (1990) (restrictions on Third Party access to confidential customer information possessed by utilities unless customer consent is obtained or a valid warrant or subpoena is obtained for law enforcement access). In response to the new statute, the CPUC initiated a new phase of their smart grid Rulemaking to develop updated privacy rules to implement SB 1476. The CPUC held several workshops and invited many interested parties, including utilities, consumer advocates, Third Party vendors and privacy advocates to make recommendations on what new rules the CPUC should adopt to implement SB 1476 and protect customer privacy. In addition to these workshops, the parties also met on their own to develop a consensus set of privacy requirements based on the Fair Information Practice Principles (FIPPS), which formed the basis of the rules ultimately adopted by the CPUC.

On July 28, 2011, the CPUC approved Decision 11-07-056 which adopted a set of "Rules Regarding Privacy and Security Protections for Energy Usage Data."[137] These rules, based on the FIPPS, and input from parties, maintained the "primary/secondary purpose" structure adopted by SB 1476. The Privacy Rules apply to utilities, Third Party contractors of the utility, and customer authorized Third Parties who obtain data from the utility; the Privacy Rules do not

[137] D.11-07-056 at Attachment D (Privacy Rules). This decision only applied to electrical utilities, a subsequent decision, D.12-08-045 (August 23, 2012), adopted the privacy rules to cover natural gas data generated by advanced meters.

apply to Third Parties who obtain customer data from the customer.[138] The Privacy Rules direct utilities to provide customers with a notice of what data is collected, and for what purpose the data is used.[139] The Rules direct the utilities to provide this notice yearly to all customers, be available on the utilities' home page, and provide a link to the privacy notice on all email to customers.[140] The Privacy Rules also provide the customer the ability to access their usage information, and allows customers to control access to their usage information. Consistent with the FIPPS, the Privacy Rules adopt a "Data Minimization" strategy for utilities and their contractors; specifically, Third Parties should only get the data necessary to accomplish the primary purpose and should hold on to the data for only as long as reasonably necessary. The Privacy Rules also contain requirements regarding the security of customer data, a requirement to notify customers and the CPUC upon a security or data breach affecting 1000 or more customers, and direct the utilities to implement periodic audits of their privacy and security practices and annually disclose the number of contractors and other Third Parties who obtain customer data.

The CPUC's Decision 11-07-056 also initiated a separate phase of the smart grid proceeding requiring investor-owned electric utilities to provide third-parties with electronic access to a customer's usage data via the utility's "backhaul" data storage and communications systems when authorized by the customer. The Third Party access must be consistent with the CPUC's privacy rules and must allow the CPUC to exercise oversight over Third Parties receiving customer data. The CPUC adopted the utility data access proposals on September 19, 2013.[141] This decision adopts a process for the oversight of Third Parties that obtain customer usage information from the utility via these utility processes. In order for a Third Party to obtain customer usage information, the Third Party must show 1) that the Third Party has obtained the customer's authorization, 2) the Third Party must meet the technical requirements of the standard, 3) acknowledge receipt of the utility tariffs and applicable rules, and 4) are not otherwise prohibited by the CPUC from receiving information. The process allows for a utility to notify the CPUC of a potential violation of the CPUC's privacy rules, whereby the CPUC will initiate an investigation of the utility's claims. Access to customer usage information will continue unless the CPUC finds the Third Party in violation of the CPUC's rules, whereupon access to customer usage information by that Third Party will cease. Additionally, a Third Party found in violation of the CPUC's rules will be identified as a company ineligible for obtaining customer usage information. Finally, this decision adopted a modified customer information service request form for those parties seeking only usage information.

Colorado's development of new customer privacy rules involved similar collaborative aspects. In November of 2010, the Colorado Public Utilities Commission (CoPUC) filed a notice of proposed rulemaking (NOPR) with the stated goal of establishing a substantial, thoughtful, and

---

[138] In 2013, California adopted AB 1274, codified at California Civil Code Section 1798.98-99, which provides privacy protection of customer usage data over Third Parties not covered by the CPUC's rules or SB 1476.

[139] Data covered by the rules is defined as "any usage information obtained through [an advanced meter] when associated with any information that can reasonably be used to identify an individual, family, household, residence, or non-residential customer." Privacy Rules at Section 1(b).

[140] For example, PG&E's Privacy Policy and "Notice of Accessing, Collecting, Storing, Using and Disclosing Energy Usage Information" can be found at http://www.pge.com/en/about/company/privacy/customer/index.page [accessed 8/11/2014].

[141] California Public Utilities Commission, In the Matter of Pacific Gas and Electric Company for Adoption of its Customer Data Access Project, et al., Decision 13-09-025 (September 19, 2013).

proactive privacy regime for the protection of customer data.[142] In response to initial comments from stakeholders to its NOPR, the CoPUC staff convened nine public workshops and one public hearing where stakeholders discussed the proposed rule language, proposed edits the language, raised related issues and debated their relative merits. At the end of this process, a proposed set of rules was filed in the proceeding that reflected either consensus of the entire group, or agreement from a majority of the involved stakeholders. Individual stakeholders then filed comments on the specific rule provisions and participated in further public hearings. These comments and testimony was considered by the administrative law judge (ALJ), which proposed a recommended decision on the rules for consideration by the CoPUC. The CoPUC adopted final rules on October 26, 2011, and those rules were effective February 14, 2012.

The CoPUC focused on the balancing of two competing but valid interests: (1) protecting the privacy interests of customers; and (2) developing a mechanism where customer-specific energy usage data could be provided to local governments, Third Parties and commercial interests. In the recommended decision adopting the new rules the ALJ found that, "(t)he bedrock for issues arising from innovations regarding energy usage is the direct regulatory authority over the essential utility-customer relationship. These considerations drive the appropriate adoption of policies to protect customer information from unauthorized disclosure while fostering customer access to information. Should a customer of record desire to authorize access by any Third Party, they may do so through informed consent provided for in these rules."[143] Specifically, the rules:

- Clarify that a utility is only authorized to use customer data to provide regulated utility service in the ordinary course of business (primary purpose).
- Affirm that utilities can share customer energy usage data with Contracted Agents without first obtaining customer consent, but only where such sharing is related to the primary purpose and the utility has secured an agreement with the Contracted Agents prohibiting use of customer energy usage data for a secondary purpose. Additionally, the Contracted Agent's data security procedures and practices must be equal to or greater those data security procedures and practices used by the utility. Affirm that a utility can release customer energy usage data if required by law or CoPUC rule.
- Create an annual privacy notice requirement for the utility addressing customer energy usage data use, access and release.
- Create a Commission-produced uniform customer consent form for use by customers to authorize the disclosure of customer energy usage data to Third Parties for a secondary purpose.
- Require the utility to validate the customer consent form prior to the release of customer energy usage data to a Third Party.
- Define aggregated customer energy usage data to be a minimum of fifteen customers, with no single customer representing fifteen percent or more of the total data set (15/15

[142] Colorado Public Utilities Commission, In the Matter of the Proposed Rules Relating to Smart Grid Data Privacy for Electric Utilities, 4 Code of Colorado Regulations 723-3, Docket No. 10R-799E, Notice of Proposed Rulemaking, Paragraph 5. All filings in Docket No. 10R-799E are available from www.dora.state.co.us.

[143] *Ibid.*, Paragraph 17.

rule). Notwithstanding, the 15/15 Rule, a utility would not be required to disclose aggregated data if the disclosure would compromise the individual customer's privacy or the security of the utility's system.

- Require the utility to file a tariff identifying its customer energy usage data and aggregated customer energy usage data services, and related costs for non-standard data services.
- Provide civil enforcement and civil penalties in the event customer energy usage data is released without customer authorization.

The California and Colorado privacy regulations for customer energy usage data have many similarities. However, areas of distinction include:

- **Scope:** California's rules apply to "covered information" which is defined as information obtained through the use of Advanced Metering Infrastructure that is identifiable to an individual. Colorado's rules apply to any "customer information" which is defined more broadly to apply to energy usage data and program participation, regardless of the metering technology used to collect such information.
- **Jurisdiction Over Third Parties**: The CPUC's decision asserts jurisdiction over Third Parties that obtain customer usage information from the utility, but defers a decision on whether the CPUC has authority to directly regulate Third Parties which obtain customer usage information from the customer. Since utility tariffs cover the exchange of data between the utility and a Third Party, the CPUC has authority over the utility tariffs. Subsequent legislation provides for an additional level of privacy protection over those Third Parties not covered by the CPUC's rules. In general, CoPUC did not assert jurisdiction over the data practices of Third Parties, other than to require that the utility's Contracted Agents must have security equal to or exceeding that of the utility. The customer consent form required by the CoPUC for Third Parties to obtain customer consent does, however, provide an explicit disclaimer putting customers on notice that the utility does not have any obligation to protect the data once it leaves their control.
- **Restrictions on Third Parties:** The CPUC's regulations provide that all Third Parties are limited to collecting only that data necessary to implement the purpose for which data is needed. Consistent with customer privacy rules adopted in the early 1990s, non-utility contractors and other Third Parties are also required to obtain customer consent prior to accessing customer usage information. Customer consent can be currently obtained through the use of a utility's tariffed Customer Information Service Request form, which has been in use by California utilities for twenty years for customer authorization of access to billing records. There are no direct CPUC restrictions on Third Parties that obtain data from the customer, but other California privacy laws applicable to privacy in general do apply. Colorado also places restrictions on the utility regarding the release of the customer's data. Since the utility is the ultimate gatekeeper on information, the utility is treated as the final arbiter of whether the consent forms were incomplete or non-compliant. Thus, while CoPUC does not place restrictions directly on Third Parties, there are requirements that the utility will oversee and the utility is ultimately overseen by the CoPUC.

- **Demand Side Management Programs:** California's rules provide an exception to the customer consent process for Third Parties assisting utilities or the CPUC with planning, implementing or evaluating demand side management programs, such as energy efficiency or demand response programs where authorized by the CPUC. Colorado's rules do not contain an explicit exemption for such data use, but do generally allow the utility to release customer energy usage data to comply with a CoPUC order.
- **Aggregated Data:** California defines aggregated customer energy usage data as a data set where all personally-identifiable information has been removed, and where the release will not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information. Colorado incorporates into its rules the presumption that information is sufficiently anonymous if aggregated consistent with a 15/15 Rule.
- **Dispute Process**: California provides a dispute mechanism for customers to challenge the accuracy or completeness of customer energy usage data, and to request corrections or amendments. Colorado's rules do not specifically address this type of dispute but a complaint can always be filed with the Commission if a customer has a specific concern.
- **Data Breach**: As a supplement to existing federal and California "red flag" data breach disclosure laws, California requires utilities to make contemporaneous reports of data breaches affecting 1000 or more customers to the CPUC, and to file an annual report of all such incidents each year. The CoPUC's rules do not require a data breach report to the commission, but there is a state statute covering the utility's obligation to report data breaches to impacted individuals.

APPENDIX D: RECOMMENDED PRIVACY PRACTICES FOR CUSTOMER/CONSUMER SMART GRID ENERGY USAGE DATA OBTAINED DIRECTLY BY THIRD PARTIES

D-1 Preamble

The Customer/Consumer Energy Usage Data Privacy Protection team under the Privacy Subgroup has developed the following recommended privacy practices for application to energy customers and the Third Parties with whom they share Customer/Consumer Energy Usage Data (CEUD). While the work of this group began early in 2011, the bulk of the work on these recommended privacy practices occurred after the California Public Utilities Commission (CPUC) issued its smart grid data access rules, the North American Energy Standards Board (NAESB) released its guidelines (REQ 22) on this subject, and the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) group released their recommendations. Those efforts applied to utilities and Third Parties obtaining access to data from those utilities. The purpose of this group's effort was to apply the same type of recommended protections to Third Parties that gain access to CEUD directly from customers or customer-owned devices, bypassing the utility and the smart meter. The goal of the group was to expand upon the good work already done.

These are recommended privacy practices that should be implemented in a comprehensive manner and not considered individually. If individual recommendations are taken out of context, they may not stand on their own. While there may exist uncertainty over the extent to which any one government agency has regulatory oversight of Third Parties using CEUD, many agree that energy usage data (that will soon become more prevalent as the electric grid gains increased intelligence) can potentially be sensitive, privacy-impacting, data in need of protection. This is particularly true when CEUD is combined with other data, such as an account number or AMI IP address,that then makes it identifiable to one premise or customer. These recommended privacy practices seek to provide suggestions as to how CEUD, and the data combined with it as just described, is best protected in order to protect personal privacy.

D-2 Definitions

Customer: Any entity that takes electric service for its own consumption.

Third Party: An entity — other than the electric utility or other electricity provider for a given premise, the applicable regulatory authority, an independent system operator (ISO) or another regional entity— that performs services or provides products using CEUD. This definition does not include Contracted Agents of an electric utility or electricity provider.

Contracted Agent: An entity under contract with the Third Party to perform services or provide products using CEUD. In some industries, Contracted Agents are referred to as Business Partners or Business Associates.

Customer/Consumer[144] Energy Usage Data (CEUD): Energy usage information and data identifiable to a premise or an individual customer obtained without the involvement of the utility.

Privacy Use Case: A method of looking at data flows that will help Third Parties to rigorously track data flows and the privacy implications of collecting and using data, and will help the organization to address and mitigate the associated privacy risks within common technical design and business practices. Use cases can help smart grid architects and engineers build privacy protections into the smart grid.

D-3 Recommended Privacy Practices

D-3.1 Privacy Notices

When a Privacy Notice Is Issued

- Prior to sharing CEUD, Third Parties should provide clear and conspicuous[145] notice to customers regarding data treatment and that CEUD will not be disclosed to other Third Parties unless authorized by the customer (with all exceptions listed).

- Notice to the customer of all intended disclosures should be re-issued at least annually.

- Re-issue should occur when significant changes are made to operational or organizational structure of the company that may impact privacy or security of the data. A few examples may include:

    1) a merger or acquisition of the company

    2) when declaring bankruptcy[146]

    3) when services are outsourced, which were not previously.

- Re-issue should also occur when major changes occur within the organization that may reasonably impact the company's data privacy practices relating to disclosing CEUD to Third Parties or Third Party's Contracted Agents, such as when new applicable laws and/or regulations become effective.

[144] There may be a legal issue in terms of who has access to this data. There may be situations in which the Customer and the consumer are not the same and that one might want to restrict access to the CEUD. These recommended practices are not designed to determine legal issues.

[145] For one example of what is considered "clear and conspicuous," see the Federal Trade Commission's document entitled "Dot Com Disclosures: Information About Online Advertising," page 5, at http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.

[146] http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=2180, and http://epic.org/privacy/airtravel/clear/.

- Customer notice should come from the Third Party with which the customer has a business relationship. Any entity that is not directly involved with the transaction being considered need not send a separate notice.[147]

What Should Be Included In a Privacy Policy Notice

- Privacy policy notices should include information about how the Third Party will access, collect, use, store, disclose, retain, dispose of, and safeguard CEUD.

- Information about data access that will or may be given to a Third Party's Contracted Agent should be provided in the initial notice to the customer. The notice may be listed by service (e.g., data formatting, billing) instead of contractor's company name.

- Separate notice should not be necessary for the sharing of CEUD with a Third Party's Contracted Agent, unless the purpose is materially different than has been previously authorized.

- Third Parties should provide customers with a process for addressing their CEUD privacy complaints. This process, which may include existing procedures established or approved by the applicable regulatory authority or other legal requirements, should be discussed in the notices to the customer.

- A customer's right to revoke authorization should be reiterated in the periodic privacy notice sent to customers.

- Breach notification processes should be communicated to customers by the Third Party as part of the periodic privacy notice.[148]

- All information privacy policies regarding disclosure to other Third Parties or the Third Party's Contracted Agents should be clear, concise (notice should be no longer than is necessary to convey the requisite information), understandable, and easily accessible.

D-3.2 Customer Authorization for Disclosures

- Data should not be disclosed to other Third Parties unless there is an authorization to do so by the customer. This authorization should notify the customer of the identity of the other Third Parties.

- When the Third Party obtains the customer's authorization, it should identify any choices available to the customer regarding CEUD disclosure as part of the authorization process (e.g., the ability to opt-out of disclosure).

[147] This is to clarify who among the common actors (Third Parties and Contracted Agents) needs to send a privacy policy notice to Customers.

[148] It is assumed that companies will comply with relevant breach notification laws. This is to make certain that a description of what the Customer should expect if a breach occurs is conveyed to the Customer.

Disclosure to Contracted Agents

- Third Parties and Third Party's Contracted Agents do not need further customer authorization in order to provide services or products, or to fulfill other obligations to customers, that have already been authorized by the customer.[149]

- Before releasing CEUD to a Third Party's Contracted Agent, Third Parties should receive confirmation that the Third Party's Contracted Agent has security and privacy safeguards in place at least equal to those implemented by the Third Party.

Customer Access to Their Data

- A Third Party should develop and communicate processes for a customer to have access to their CEUD and to be able to request that the CEUD be corrected where inaccuracies exist. The process for gaining data access should be a relatively simple process for the typical customer. This process, which may include existing procedures established or approved by the applicable regulatory authority or other legal requirements, should be discussed in the notices to the customer. The data provided to the customer should be provided in a form that is reasonably understandable by the average customer.

Customer Authorization & Data Accuracy

- Third Parties should provide customers with reasonable mechanisms for:
    1) granting and revoking authorization for access to their CEUD;
    2) providing feedback regarding the disclosure of CEUD; and
    3) requesting corrections to the CEUD.

D-3.3 Data Disclosure

- CEUD collected by a Third Party should be limited to only that data necessary to fulfill the purpose specified in the customer's authorization[150].

- A separate customer authorization should be obtained before CEUD is used in a materially different manner than previously authorized.

Aggregated or De-identified CEUD[151]

- If the customer has already authorized a particular service or product, and a Third Party or Third Party's Contracted Agent needs to disclose aggregated or de-identified information in order to produce that service or product, the Third Party or Third Party's Contracted Agent should not need a new authorization to disclose the aggregated or de-

[150] There may be a legal issue in terms of who has access to this data. There may be situations in which the Customer and the consumer are not the same and that one might want to restrict access to the CEUD. These recommended practices are not designed to determine legal issues.

[151] There are currently no known standards for determining what constitutes de-identified CEUD. The typical intention is that all identifying information has been removed.

identified information so long as that information cannot be tracked back to an individual or used to identify a customer.

- Third Parties should specify that any other Third Party or Contracted Agent receiving CEUD that has been anonymized or de-identified should not attempt to re-identify the data or otherwise identify an individual premise or customer.

Legal Disclosure for Law Enforcement

- Third Parties should have procedures in place to provide data access to law enforcement when presented with legal obligations to do so. These procedures should include validation that the necessary legal requirements have been met (e.g., subpoena, court order, etc.).

Disclosure of Information in Situations of Imminent Threat to Life or Property

- These practices do not apply to emergency disclosures of information provided to emergency responders in situations involving an imminent threat to life or property. What constitutes an emergency disclosure should be determined by appropriate authorities.

D-3.4 Customer Education & Awareness

- Third Parties should develop and implement customer education and awareness plans to inform the relevant customers about the Third Party's CEUD privacy protection policies and practices.

- The Third Party should provide its customers with educational and awareness materials that summarize the steps that the organization is taking to reduce potential risks associated with unauthorized use of CEUD, and describe the steps that customers can take to help reduce their own risk.

- The customer should be made aware that CEUD may unavoidably differ somewhat from different sources based on such factors as differences in technology, timing, and validation. For example, potential exists that data from a HAN device may differ from an aggregated view provided by a utility.

D-3.5 Data Minimization

- Collection of CEUD by Third Parties should be limited to only that information necessary to fulfill the purpose (e.g., to provide a service or product, etc.) as set forth in the customer's authorization.

D-3.6 Data Quality

- Third Parties and Third Party's Contracted Agents using CEUD should endeavor to ensure that the data is accurate and complete. It should be recognized that the data is only as accurate and complete as the information received if the holder is not the original collector. This should not preclude a Third Party or Third Party's Contracted Agents from modifying or enhancing CEUD, provided that it is clear that modifications or enhancements have been made when such information is disclosed.

D-3.7 Data Security & Governance

- Third Parties should protect information under their control from unauthorized access, copying, modification, inappropriate disclosure, or loss by having information privacy protections in policies, procedures, and practices relating to data security and to disclosure and accuracy of data disclosed to the Third Party's Contracted Agents, or to other Third Parties.

- These policies or procedures should periodically be reviewed, assessed, and updated, as necessary, to ensure CEUD is properly addressed.

- Third Parties should appoint positions and/or personnel to ensure that security and privacy policies are properly maintained, updated, and followed.

- Privacy practices should be transparent.

D-3.8 Privacy Practices Risk Assessment

- Third Parties should conduct and document periodic privacy impact and risk assessments and analyses associated with their processes for disclosing CEUD to Third Party's Contracted Agents. They should use these risk analyses and privacy impact assessments to update, when appropriate, the applicable policies and practices. Such risk analyses and privacy impact assessments should be considered at least annually or when:

  - Major changes occur within their organization that may reasonably impact the company's data privacy practices relating to disclosing CEUD to Third Parties or Third Party's Contracted Agents;
  - New applicable laws and/or regulations become effective;
  - An event related to the unauthorized disclosure of CEUD occurs at the company; and
  - Any other circumstance occurs that the Third Party or Third Party's Contracted Agent determines warrants such risk analysis.

- Third Party's Contracted Agents should conduct similar analyses and provide the results of their analyses/assessments to the Third Party in a timely manner.

- In developing and updating policies and practices, Third Parties should develop a set of Privacy Use Cases as a method to track information flows and the privacy implications of collecting and using data to help the organization to address and mitigate the associated privacy risks within common technical design practices and business practices.[152]

- Third Parties should share solutions to common privacy-related problems with other smart grid market participants in some appropriate manner (e.g., trade forums, associations, public policy, public out-reach, external coordination, etc.).

[152] For an example of smart grid use cases, see NISTIR 7628 Rev. 1 Volume 3, Chapter 10.

D-3.9 Data Retention and Disposal

- Unless authorized differently, Third Parties should keep CEUD no longer than is necessary to fulfill the business purposes for which it was collected, and as reasonably interpreted to be required to comply with legal or regulatory requirements.

- If CEUD is to be used for research, then policies and procedures should be established for retention and de-identification related to these activities.

- Third Parties should inform the customers of their data retention policies as part of their notice to customers.

- Third Parties' data retention policies should include when and how data should be irreversibly disposed of, including after revocation of a customer's authorization to collect or keep CEUD.

D-3.10 Data Breaches

- Third Parties should identify any state or federal requirements for disclosure or data breach notification that may be applicable to a Third Party or Contracted Agent.

- Consider including CEUD as data that may require a notice for any unauthorized breach dependent upon the granularity of the data and applicable legal breach notification requirements.

D-3.11 Employee Training

- Third Parties and Third Party's Contracted Agents should develop, disseminate, and periodically review and update a formally documented security and privacy awareness and training policy (which specifically includes the protection of CEUD) with documented supporting implementation procedures.

- The organization should document, maintain, and monitor each employee's security and privacy training activities on an individual basis, including basic security and privacy awareness training in accordance with the organization's security and privacy policies.

D-3.12 Audits

- Each Third Party should conduct a periodic independent audit of Third Party's data privacy and security practices.

- Each Third Party should periodically verify the privacy and security practices of Third Party's Contracted Agents. This may occur in one or more ways. Some examples are:

    1. Conducting an audit of the Third Party's Contracted Agents' privacy and security practices.
    2. Requiring the Contracted Agent to provide Third Party with an independent audit of its privacy and security practices.

3. Examining the results of an independent audit[153] of the Third Party's Contracted Agents' privacy and security practices.
4. Examine the results of a recent SSAE-16[154] audit.
5. Review any existing Information Security Management System (ISMS)[155] certifications.
6. Review any recent privacy impact assessments that have been performed.

[153] "Independent Audit" is described in F. Gallegos, "IT Audit Independence: What Does it Mean?" *ISACA Journal* vol. 6, 2003, http://www.isaca.org/Journal/Past-Issues/2003/Volume-6/Pages/IT-Audit-Independence-What-Does-It-Mean-.aspx [accessed 8/11/2014]. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.

[154] Statement on Standards for Attestation Engagements (SSAE) No. 16 replaced the SAS70 Type II audit. "SSAE 16 is an attestation standard geared towards addressing engagements conducted by practitioners (known as "service auditors") on service organizations for purposes of reporting on the design of controls and their operating effectiveness." See more in C. Denyer, "SSAE 16 | Introduction to Statement on Standards for Attestation Engagements (SSAE) No. 16," in *The SSAE 16 Resource Guide*, NDB LLP, http://www.ssae16.org/what-is-ssae-16/introduction-to-ssae-16.html [accessed 8/11/2014].

[155] A certified Information Security Management System (ISMS) is described at "ISO/IEC 27001 Information Security Management," *BSI Group* [Web page], http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/ISO-IEC-27001/ [accessed 8/11/2014].

APPENDIX E: PRIVACY USE CASES

Category: AMI	Privacy Use Case #1
Scenario: Meter sends information	

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

A meter sends automated energy usage information to the Utility (e.g. meter read (usage data). The automated send of energy usage information is initiated by the meter and is sent to the Advanced Metering Infrastructure (AMI) Head End System (HES). The HES message flows to the Meter Reading and Control (MRC). The MRC evaluates the message. The MRC archives the automated energy usage information and forwards the information onto the meter Data Management Systems (MDMS).

- Meter configuration information
- Periodic meter Reading
- On-Demand meter Reading

Net metering for distributed energy resources (DER) and plug in electric vehicle (PEV)

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Enables new products, services and markets • Optimizes asset utilization and operates 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 • Third Party or party acting as an agent of the utility access to energy usage information for market and/or consumer services • Third Party or party acting on behalf of the utility reliable data • Customer data access • Reliable data for billing

1.1	**Data Privacy Recommendations** Any individually negotiated purchase agreement that contains or is associated with personally identifiable customer data should be subject to the same privacy and security applications as personally identifiable data.
1.2	Meter read data should be evaluated to determine if it should be protected data regardless of type of service or tariff or scheduled meter read frequency and the same policy notice can apply. Similarly, the same choice and consent information can be used across all scenarios noted above, with the caveat that if any Contracted Agents are involved, the individual has been notified and consented to the Contracted Agent's access to the data identified as necessary for that activity. This notice may happen within the initial privacy notice given at account set up.

1.3	Customer access to data in real-time or near-real-time, particularly for net metering/feed in tariff (FiT) data is important for many customers to optimize performance of assets that generate or store electricity. This access should be limited to the consumer associated with the meter, the utility for operational and billing purposes or their authorized agents, and consumer-authorized Third Parties. (The OECD principle for access indicates that individuals should have access to data associated with them.)
1.4	Meter reading is an ongoing activity, so it is important that utilities create a monitoring and enforcement process that ensures compliance on a continuous basis.
1.5	Utility-authorized agents and/or Third Parties may be given access to meter reading data for various customer peer performance/comparison purposes. These agents or Third Parties should also conform and comply with utility privacy policies, and customers should consent to the disclosure of their information to these agents or Third Parties.

	AICPA Principle	Applies: X	Notes
1.6	**Management Principle**	X	An individual, team or department should be assigned responsibility for ensuring policies and procedures exist that cover the situations involved within this use case scenario.
1.7	**Notice Principle**	X	Should be provided for all meter reading, regular consumption and net metering scenarios.
1.8	**Choice and Consent Principle**	X	Ensure that when customers sign up for service that this choice and consent requirement is met.
1.9	**Collection Principle**	X	Over time, data collection may change as new applications, technologies, or correlations of data are made available. Utility policy should indicate that collection purposes may change over time and that utilities will notify customers of any proposed changes that may impact collection in order to secure an updated choice and consent.
1.10	**Use and Retention Principle**	X	Retention may be impacted by time frames to record and compensate for net metering scenarios. Data retention may also be impacted by local, state, or federal laws/regulations/requirements outside of utility operational needs.
1.11	**Access Principle**	X	Access to the meter usage data, and any associated data that could reveal personal data, should be limited to only those who need such access to perform their job activities.
1.12	**Disclosure to Third Parties Principle**	X	Utility net metering payments to customers may be considered revenue or income and thus subject to tax laws, or garnishments for child support, legal claims, etc. Requests may come from law enforcement agencies or other entities that make requests for information from utilities. Some of the legal implications may not require implicit or explicit consent.

1.13	**Security for Privacy Principle**	X	Safeguards should be applied as appropriate to mitigate associated risks to an acceptable level.[156]
1.14	**Quality Principle**	X	Controls should be established to ensure meter usage data is as accurate as necessary for the purposes for which it is being collected.
1.15	**Monitoring and Enforcement Principle**	X	This should not be just a once and done audit on a yearly basis since meter reading is an ongoing activity. Utilities should create a practice of regular compliance monitoring on a rolling basis to completely cover the customer records on a several times a year frequency.

[156] For more discussion on identifying and selecting applicable security requirements for a smart grid information system, see Chapter 3, High-Level Security Requirements.

Category: AMI	Privacy Use Case #2
Scenario: Utility sends operational command to 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, utility-authorized agents, 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

A utility requires an operational command be sent to the meter, such as a disconnect or reconnect of an electric smart meter. The command flows to the Meter Reading and Control (MRC) that looks up the meter associated with the customer and then instructs the Advanced Metering Infrastructure (AMI) Head End System (HES) to communicate the command to the meter. The HES evaluates current conditions and, if suitable (e.g. reconnects are not executed if the system is in a rolling black out state), sends the command to the meter. When the meter receives the command and parameters, the meter evaluates the command as to whether it is permitted. If the command is permitted, the meter executes the command and sends the result to the HES. If the command is not permitted, the meter sends the result to the HES. The HES evaluates the result (whether the action was successful or not and why) and relays that to the MRC. The MRC records the command result and notifies the appropriate actors.

- Configuration request
- Calibration request
- Connect Disconnect request
- Prepaid metering configuration/setup

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters	• Integrity of control commands to the meter is critical to avoid dangerous/unsafe connections. Availability is not important with the exception of situations such as fire or medical emergency for remote connect/disconnect. • Confidentiality requirements of the meter command is generally not very important	• Customer Safety • Third Party or party acting as an agent of the utility access to energy usage information for market and/or consumer services

2.1	**Data Privacy Recommendations** Utilities collect personal data that includes customer name and address/location to establish an account, and this information is associated with a meter number. This personal data should be restricted to those software applications and resources that require this information to associate meter location and billing information. The security safeguard principle has specific application here. Information about data access that will or may be given to a Contracted Agent should be provided in the initial notice to the customer. The notice may be listed by service (e.g., data formatting, billing) instead of contractor's company name. Separate notice is not necessary for the sharing of CEUD with a Contracted Agent, unless the purpose is materially different than has been previously authorized.
2.2	Any connect or disconnect event should be identified by the meter number and completely disassociated with any personal data (i.e., it is not John Smith's meter that is turned on/off, rather, it is meter number 123456 that is the subject of an action). This avoids the transmission of personal data across the AMI network.

2.3	The data quality principle applies - customers need the ability to review and update their personal data as the parties who are responsible for payments may change over time.
2.4	Special consideration must be given to situations where collection of past due amounts is done by a Contracted Agent. Utilities should provide easy to understand statements as part of the connect/reconnect process that outlines any role of Contracted Agents such as collection agencies. Utilities should ensure that their Contracted Agents, and any Third Parties, are handling personal data with the same levels of privacy safeguards as conducted by utilities themselves.
2.5	To a great extent, the effect of Prepaid AMI on Privacy is dependent on the details of implementation. For example; o Were the meter itself capable of performing the "countdown" of the amount of prepaid service remaining, then the utility might not have to collect any usage data. The utility could simply update the meter with the amount of service prepaid, and the meter itself could track remaining service, and shut service off if the prepaid amount were exceeded. o On the other hand, if the "countdown" were handled in the utility backend systems, quite granular usage data collection may be required. Prepaid metering has the potential to reduce the number of utility/consumer transactions – specifically connect/disconnect transactions that could potentially expose personal data during each transaction as well as utility need to conduct credit checks and/or maintain records on account deposits. As a new practice for almost all utilities, care should be exercised in the definition of new processes and procedures to ensure that data privacy principles are enacted.
2.6	The simple fact of whether a customer was on a Prepaid tariff could be seen as information that a customer would want protected. However, this may be no different in effect from the desire of commercial and industrial customers to keep their operating costs confidential.

	AICPA Principle	**Applies: X**	**Notes**
2.7	**Management Principle**	X	Maintain policies that oversee the implementation and compliance with the related privacy and security policies to protect the data involved with this use case.
2.8	**Notice Principle**	X	Information about data access that will or may be given to a Contracted Agent should be provided in the initial notice to the customer. The notice may be listed by service (e.g., data formatting, billing) instead of contractor's company name. Separate notice is not necessary for the sharing of CEUD with a Contracted Agent, unless the purpose is materially different than has been previously authorized.
2.9	**Choice and Consent Principle**	X	Identify if personal data may be used for billing and collections as part of a connect/disconnect process.
2.10	**Collection Principle**	X	Personal data is required for billing purposes, but should be protected and maintained per management principle.
2.11	**Use and Retention Principle**	X	Data involved should only be retained for as long as necessary to perform the associated business activities.

2.12	**Access Principle**	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
2.13	**Disclosure to Third Parties Principle**	X	May be shared with Contracted Agents if these are used for authorized purposes. Disclosure to Third Parties should not occur without consent consistent with the data privacy recommendations (Appendix D: Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties).
2.14	**Security for Privacy Principle**	X	Financial information has particular sensitivity, and utility procedures regarding protection of personal data and financial information should limit physical and electronic access on a “need to know” basis by implementing appropriate policies and technical safeguards.
2.15	**Quality Principle**	X	Utilities must ensure that they have correct and accurate contact information if accounts are sent to collections, and to ensure that any disconnects are targeted to the right meters.
2.16	**Monitoring and Enforcement Principle**	X	Access logs should be generated and regular audits of those logs should occur.

Category: AMI	Privacy Use Case #3
Scenario: Utility sends non-operational instruction to meter (peer-to-peer)	

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

This use case describes the Utility sending a non-operational instruction send to meter as a peer-to-peer transaction. A Utility requires actions from a set of meters which may or may not result in a change to the power state of the grid. These include at least meter reading, and certain configuration changes. The Meter Reading and Control (MRC) determines the need to send instruction(s) to a meter. The MRC looks up the meter associated with the customer and then instructs the Advanced Metering Infrastructure (AMI) Head End System (HES) to queue up and execute the instruction(s). The AMI Head End can determine the instruction needs to be split into packets, schedules the sending of the packets and continues to send the packets to the meter until all instruction packets have been sent. The meter receives the instruction(s) and determines if the instruction is permitted. After execution, the meter sends the instruction result to the HES. The HES will then send the instruction result to the MRC. If the instruction result is energy usage information, the MRC will then forward the energy usage information onto the Meter Data Management System (MDMS). If the MDMS receives energy usage information, then the MDMS forwards the energy usage information onto other actors for other actions.

1. Meter calibration validation
2. Connectivity validation
3. Geolocation of meter
4. Smart meter battery management

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters • Increases the timeliness, availability, and granularity of information for billing	• Confidentiality may or may not be an issue depending on whether information is public (date, time) or private (password change, Personally Identifiable Information). Some items must be confidential due to laws and regulations; confidentiality of other items, such as firmware or GPS coordinates, may be left up to local policy, • Integrity of meter maintenance repairs and updates is essential to prevent malicious intrusions • Availability is important, but only in terms of hours or maybe days to provide synchronization and coherence of devices on the network, i.e. all devices acting together for entire population	• Customer data privacy and security • Third Party or party acting as an agent of the utility having access to customer & Utility information • Third Party access to electrical distribution system, e.g. separation of duties & authority (regulatory impact) • Vendor product quality

3.1	**Data Privacy Considerations**

	The Customer Information Systems (CIS), Meter Data Management Systems (MDMS) and Outage Management Systems (OMS) may contain multiple types of personal data that may be impacted by meter reading and configuration changes or updates. Utility resources and authorized Third Parties should follow utility privacy policies to safeguard any personal data, including energy usage data. For example, a connectivity ping that is negative may trigger a request to an OMS and/or workforce management system to schedule an onsite repair visit. Personal data in the form of customer name and address would be needed to schedule that repair with utility or authorized Contracted Agents. That connectivity ping may also generate a report identifying unresponsive meters. Care should be exercised to minimize personal data that appears in these reports, and limits on the access to these reports by resources trained in privacy policies and practices.
3.2	Care should be exercised to ensure authorized Third Parties or other service providers do not have unnecessary access to customer information that is not required for completion of their responsibilities.
3.4	The personal data in any report should be kept to a minimum to limit privacy risk, particularly data that could unintentionally provide a potential exploit or expose a vulnerability. Data should be limited to only the minimum necessary to effectively aid the appropriate utility or Contracted Agent workers in completion of their responsibilities.
3.5	Utility repair and maintenance teams may have name/address/location associated with meters. Utility teams may include Contracted Agents that are subcontractors to utilities or even subcontractors to utility subcontractors, so all processes should be evaluated to determine what, if any, personal data is required to complete their responsibilities. When personal data is required, all resources should be trained to safeguard the data from unauthorized exposure, display, or updates to that data.
3.6	Associating meter data with personal data can create privacy risks. Meter number is associated with personal data in one or more systems – CIS being the most likely application. Care must be exercised by field resources who may have printouts, smart device displays, or laptop displays that contain customer personal data. Any reports on these non-operational activities should be assessed from a privacy perspective to ensure that if any personal data is included that appropriate safeguards are taken to limit exposure to authorized utility or Third Party resources.
3.7	Data used to specify location could reveal personal data associated with the location. Determine what data is used in any reports and who has access to these reports in digital or print formats. Location-based information may be considered privacy information itself.
3.8	Access to personal data should be limited to only that necessary to accomplish individual job responsibilities.
3.9	Different applications keep information for differing periods of time. CIS might keep data about outages that impacted a specific customer in that specific customer's file for a long time. Some historical data can be very helpful to identifying future maintenance needs, assess equipment performance, or determine meter upgrade schedules. This data may be indefinitely held, but should be anonymized, i.e. stripped of personal data, so that personal data is associated with a meter number but not personal data or energy usage information.
3.10	Assess how long any reports generated on non-operational activities are retained. Create policy safeguards for any reports that must contain personal data.

	AICPA Principle	Applies: X	Notes
3.11	**Management Principle**	X	Policies and procedures should exist for the data collected, used, shared and stored for non-operational meter reading, configuration, or other activities. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed, including during exception processing such as an outage.
3.12	**Notice Principle**	X	Customers should be given notice about the types of data involved in these meter activities if their personal data is involved, and the policies and procedures that are in place for protecting the information and using it appropriately.
3.13	**Choice and Consent Principle**	X	Customers should be given choices, as feasible, about how communications with them are made regarding any outreach required as part of these non-operational activities. They should also be asked during initial account setup for consent to share their data with any Contracted Agents or Third Parties, and consent to having their data retained to allow for historical statistical analysis.
3.14	**Collection Principle**	X	Only the data necessary to effectively and efficiently support any activity should be collected, used, or reported as part of non-operational meter functions.
3.15	**Use and Retention Principle**	X	The data collected for any non-operational activities should be used only for the purpose set forth in the customer's authorization. Personal data collected or generated that is not necessary to fulfill the purpose set forth in the customer's authorization, should be deleted as soon as possible upon completion of the meter task.
3.16	**Access Principle**	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
3.17	**Disclosure to Third Parties Principle**	X	Data collected or created during performance of non-operational meter tasks should not be shared with any Contracted Agents or Third Parties unless there is an authorized processing need for such sharing, and if the customer has given consent for the information to be shared. During planned or unplanned meter activities, select customer data may be shared with Contracted Agents for purposes of maintenance and repair of meters.

3.18	**Security for Privacy Principle**	X	All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
3.19	**Quality Principle**	X	Controls and processes should be in place to ensure data is kept accurate as it is collected, and as it is updated during performance of meter activities.
3.20	**Monitoring and Enforcement Principle**	X	Processes should be in place to monitor compliance with the privacy policies and procedures related to collecting, storing, using, sharing and retaining data. Utilities may consider conducting a privacy audit whenever any changes to these non-operational meter activities are enacted. Procedures should exist to address privacy-related inquiries and disputes from customers involved in any non-operational activities involving meters.

Category: AMI	Privacy Use Case #4

Scenario: Field tool sends instruction to the 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

A field tool requires onsite maintenance of an electric smart meter. The Field Tool connects directly to an electric smart meter, then the command flows to the smart meter. When the meter receives the command and parameters, the meter evaluates the command as to whether it is permitted. If the command is permitted, the meter executes the command and sends the result back to the field tool. This use case is a closed loop, as stated in the preconditions.

- Meter calibration update
- Meter configuration update

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables new products, services and markets • Optimizes asset utilization and operate efficiently	• Confidentiality is not important unless some maintenance activity involves personal information • Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions and integrity of billing data to prevent high utility bills • Availability is important, because field tool requires real time interaction with the meter.	• Customer data privacy and security • Third party or party acting as an agent of the utility having access to customer & Utility information

4.1	**Data Privacy Recommendations** Utilities collect personal data that includes customer name and address/location to establish an account, and this information is associated with a meter number. This personal data should be restricted to only authorized purposes. The security safeguard principle has specific application here.
4.2	Utilities should review their policies regarding notifications to customers of planned and unplanned meter maintenance to ensure that any personal data is managed to minimize unnecessary exposure to utility resources, and that any resources that have access to this information have appropriate training to safeguard data privacy. What is “unnecessary exposure” will need to be determined by each utility based upon their organization, location and associated requirements.
4.3	Any maintenance event should be identified by the meter number and completely disassociated with any personal data, so it is not John Smith’s meter that is subject to maintenance, but it is Meter number 123456 that is the subject of an action. This avoids the transmission of personal data across any utility network.

	AICPA Principle	**Applies: X**	**Notes**
4.4	**Management Principle**	X	Maintenance policies should exist and be followed as part of the new account setup and outline how

			personally identifiable information is used in maintenance processes.
4.5	**Notice Principle**	X	Notice that a power company employee might need access to physical premises is required.
4.6	**Choice and Consent Principle**	X	Initial set up of a customer account should include utility statements about meter maintenance, as well as other utility assets, and should secure customer acceptance of scheduled and emergency maintenance procedures at that time.
4.7	**Collection Principle**	X	Establish the collection policy during the new account process, or update existing policies to indicate how personally identifiable information may be used in any meter maintenance process.
4.8	**Use and Retention Principle**	X	Meter maintenance may entail direct contact with customers at their homes or work locations. Maintenance resources in the field may have personally identifiable information about customers to establish their validity as authorized representatives of the utility. Utility processes should incorporate practices to minimize exposure of customer information and delete the information from field equipment and related systems as soon as the full maintenance operation is completed.
4.9	**Access Principle**	X	Meter maintenance should not change this general utility policy. It has particular relevance if meter maintenance is triggered by a change in customer account that requires a change in the meter itself. Customers may wish to review their information for accuracy in these situations where a meter has been changed to ensure that all personal data regarding the new meter is correct. Access to personal data should be limited to only those with a specific job responsibility requiring such access.
4.10	**Disclosure to Third Parties Principle**	X	Any Contracted Agents performing maintenance on behalf of the utility must comply with all utility data privacy policies.
4.11	**Security for Privacy Principle**	X	Meter maintenance may impact cybersecurity settings in a meter, so utilities should institute practices that fully test any proposed updates on all relevant models of meters prior to field implementation.
4.12	**Quality Principle**	X	This is relevant to ensure that any changes to a meter (update, upgrade, change to different meter to support net metering, etc.) reflect accurate information.
4.13	**Monitoring and Enforcement Principle**	X	Conduct a test or audit of privacy protections on a random statistically valid sampling of meters after a maintenance procedure such as a meter upgrade or change impacting a statistically significant number of meters.

Category: AMI	Privacy Use Case #5

Scenario: Utility sends batch instruction to meters (group multicast transaction)

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 use case describes a batch instruction send to meters as a multicast transaction in an open loop situation. The open loop situation means that Advanced Metering Infrastructure (AMI) Head End System (HES) does not expect a response for each packet sent to a meter. A Utility requires actions from a set of meters which may or may not result in a change to the power state of the grid. These include at least meter reading, and certain configuration changes. The Meter Reading and Control (MRC) determines the need to send batch instructions to more than one meter. MRC looks up the meter associated with the customer and then instructs the Advanced Metering Infrastructure (AMI) Head End System (HES) to queue up and execute the instructions. The AMI Head End can determine the instruction needs to be split into packets, schedules the sending of the packets and continues to send the packets to the meters until all instruction packets have been sent. The meter(s) receive the instruction(s) and determines if the instruction is permitted. After execution, the meter(s) send the instruction result to the HES. The HES will then send the instruction result to the MRC. If the instruction result is energy usage information, the MRC will then forward the energy usage information onto the Meter Data Management System (MDMS). If the MDMS receives energy usage information, then the MDMS forwards the energy usage information on to other actors for other actions.

- Firmware update
- Key management update

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Enables new products, services and markets • Reduces cost of operations	• Confidentiality is not important unless some maintenance activity involves personal data • Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions • Availability is important, but only in terms of hours or maybe days	• Confirmation (if required) of update status. • Customer data privacy and security • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services

5.1	**Privacy Recommendations** This scenario is similar to Use Case 3, the exception being this case involves batch communications instead of single peer-to-peer communications. The Customer Information System (CIS), Meter Data Management System (MDMS) and Outage Management System (OMS) may contain multiple types of personal data that may be impacted by meter reading and configuration changes or updates. Utility resources and authorized Contracted Agents should follow utility privacy policies to safeguard any personal and energy usage data. For example, a failed update ping may trigger a request to an OMS and/or workforce management system to schedule an onsite repair visit. Personal data in the form of customer name and address would be needed to schedule that repair with utility or authorized Contracted Agent resources. Care should be exercised to minimize personal data that appears in these reports, and limits should be put on the access to these reports by resources trained in privacy policies and practices.
5.2	Care should be exercised to ensure authorized Contracted Agents or other service providers do not have unnecessary access to customer information that is not required for completion of their responsibilities.

5.3	The personal data in any report should be kept to a minimum to limit privacy risk, particularly data that could unintentionally provide a potential exploit or expose a vulnerability. Data should be limited to only the minimum necessary to effectively aid the appropriate utility or Contracted Agent workers in completion of their responsibilities.
5.4	Utility repair teams may have name/address/location associated with meters that are subject to a non-operational activity (remote or onsite). Utility repair teams may include Contracted Agents that are subcontractors to utilities or even subcontractors to utility subcontractors, so all processes should be evaluated to determine what, if any, personal data is required to complete their responsibilities. When personal data is required, all resources should be trained to safeguard the data from unauthorized exposure, display, or updates to that data.
5.5	Associating meter data with personal data can create privacy risks. Meter number is associated with personal data in one or more systems - CIS and TCS being the most likely applications. Care must be exercised by field resources who may have printouts, smart device displays, or laptop displays that contain customer personal data. Any reports on these non-operational activities should be assessed from a privacy perspective to ensure that if any personal data is included that appropriate safeguards are taken to limit exposure to authorized utility or Contracted Agent resources.
5.6	Data used to specify location could reveal personal data associated with the location. Determine what data is used in any reports and who has access to these reports in digital or print formats. Location-based information may be considered privacy information itself.
5.7	Access to personal data should be limited to only that necessary to accomplish job responsibilities.
5.8	Different applications keep information for differing periods of time. CIS might keep data about outages that impacted a specific customer in that specific customer's file for a long time. Some historical data can be very helpful to identifying future maintenance needs, assess equipment performance, or determine meter upgrade schedules. This data may be indefinitely held, but should be anonymized, i.e. stripped of personal data, so that it is associated with a meter number but not personal data or energy usage information.
5.9	Assess how long any reports generated on non-operational activities are retained. Create policy safeguards for any reports that must contain personal data.

	AICPA Principle	**Applies: X**	**Notes**
5.10	**Management Principle**	**X**	Policies and procedures should exist for the data collected, used, shared and stored for non-operational meter reading, configuration, or other activities. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
5.11	**Notice Principle**	**X**	Customers should be given notice about the types of data involved in these meter activities if their personal data is involved, and the policies and procedures that are in place for protecting the information and using it appropriately. Customers should be given notice that their data may be made available to utilities' Contracted Agents in the course of providing electrical services.

5.12	**Choice and Consent Principle**	**X**	Customers should be given choices, as feasible, about how communications with them are made regarding any outreach required as part of these non-operational activities.
5.13	**Collection Principle**	**X**	Only the data necessary to effectively and efficiently support any activity should be collected, used, or reported as part of non-operational meter functions.
5.14	**Use and Retention Principle**	**X**	The data collected for any non-operational activities should be used only for the purposes authorized by the consumer. Personal data collected or generated that is not needed for statistical or analytical purposes, should be deleted as soon as possible upon completion of the meter task.
5.15	**Access Principle**	**X**	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
5.16	**Disclosure to Third Parties Principle**	**X**	Data collected or created during performance of non-operational meter tasks should not be shared with any Contracted Agents or Third Parties unless there is an authorized need for such sharing, and if the customer has given consent for the information to be shared. During planned or unplanned meter activities, select customer data may be shared with Contracted Agents for purposes of maintenance and repair of meters.
5.17	**Security for Privacy Principle**	**X**	All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
5.18	**Quality Principle**	**X**	Controls and processes should be in place to ensure data is kept accurate as it is collected, and as it is updated during performance of meter activities.
5.19	**Monitoring and Enforcement Principle**	**X**	Processes should be in place to monitor compliance with the privacy policies and procedures related to collecting, storing, using, sharing and retaining data. Utilities may consider conducting a privacy audit whenever any changes to these activities are enacted that relate to personal or energy usage information. Procedures should exist to address privacy-related inquiries and disputes from customers involved in any non-operational activities involving meters.

Category: AMI	Privacy Use Case #6

Scenario: Meter sends alarm or unsolicited and unscheduled request to the utility

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

A meter sends an alarm or unsolicited and unscheduled request to the Utility (e.g. Physical tamper detection, Network join request, or HAN device / direct load control device enrollment request (proxy for customer). The message is initiated by the meter and sends the messages to the Advanced Metering Infrastructure (AMI) Head End System (HES). The HES message flows to the Meter Reading and Control (MRC). The MRC evaluates the message. The MRC records the command result and notifies the appropriate actors.

Smart Grid Characteristics	Cybersecurity Objectives/Requirements	Potential Stakeholder Issues
• Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters	• Confidentiality is not important unless alarm contains private information or exposes an attempt to obtain security information stored in the meter • Integrity - Protect against energy theft Protect integrity of meter configuration Protect integrity of reporting To protect the integrity of the network (authorized devices) • Availability is important to capture last gasp detecting, join detection, and reporting	• Network Service Providers • Customer may receive outage notification through Third Party • Billing service provider • Transmission & Distribution service provider

6.1	**Data Privacy Recommendations** Utilities collect personal data that includes customer name and address to establish an account, and this information is associated with a meter number. This personal data should be restricted to those software applications and resources that require this information in processes that identify and schedule meter maintenance for the purposes authorized by the customer. The security safeguard principle has specific application here.
6.2	Utilities should develop policies regarding meter tampering/removal detection that ensure that any personally identifiable information is managed to minimize its exposure to utility resources, and that any resources that have access to this information have appropriate training to safeguard data privacy. Utilities should understand the capabilities and any security vulnerabilities of the meters that are installed to develop appropriate policies to minimize exposure of personal data at the meter itself.
6.3	Any meter message event should be identified by the meter number and address, so it is not John Smith's meter that is sending an unsolicited message, but it is meter number 123456 at a specific location that is the subject of an action.
6.4	Utilities should review their account setup policies to ensure that notice is given up front that attempts to interfere with the operations of a meter may result in civil or criminal actions, and that information may be shared with law enforcement in such situations.

	AICPA Principle	Applies: X	Notes
6.5	**Management Principle**	X	Defining the management of issues of power theft accusation and ultimate adjudication and disposition are critical. Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
6.6	**Notice Principle**	X	Utility should provide a statement in the notice that meter tampering could lead to access to meter data, including personal data, which could then result in investigation and legal actions that could have impacts on the future disposition of the account.
6.7	**Choice and Consent Principle**	X	See discussion under Recommendations, above.
6.8	**Collection Principle**	X	See discussion under Recommendations, above.
6.9	**Use and Retention Principle**	X	Use and retention of smart meter data, including data related to energy theft, should be subject to sunset and expungement requirements as set by the appropriate regulatory or legal authority. In the absence of regulatory or legal requirements, a utility may wish to consider setting requirements that are congruent with other expungement laws regarding personal data.
6.10	**Access Principle**	X	Data regarding energy theft might be requested by legal authorities, credit agencies and other utilities and vendors. Utility policies should include education and training for utility and contracted personnel regarding consistent treatment of these requests in compliance with applicable laws and regulations, as well as the AICPA principles. Access should be limited to only those with a specific job responsibility requiring such access.
6.11	**Disclosure to Third Parties Principle**	X	Organizations should have procedures in place to provide data access to law enforcement or other organizations with a legal need when presented with legal obligations to do so. These procedures should include validation that the necessary legal requirements have been met (e.g., subpoena, court order, etc.).
6.12	**Security for Privacy Principle**	X	Protection of data related to criminal theft records would need to be as securely guarded against unauthorized disclosure as personal data.

6.13	**Quality Principle**	X	The harm from inaccurate data sent by a meter - such as an incorrect tamper alarm - could be considerable. Utilities should develop policies that expunge “false positive” meter messages from customer personal data and any records that may be used for establishing financial credit or new customer deposits.
6.14	**Monitoring and Enforcement Principle**	X	Failure to monitor and enforce could result in harm to the perpetrator, the falsely accused, the energy provider and Third Parties who are inaccurately informed.

Category: Demand Response (DR)	Privacy Use Case #7

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	Cybersecurity 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

7.1	**Data Privacy Recommendations** Utilities have personal consumer information such as name, phone number and address for billing. If customer has opted for an electronic payment arrangement, the utility would also have sensitive financial data in cases of payments from consumers. The security safeguard principle has specific application here.
7.2	The use and retention principle applies - utilities should provide notification of why personal data is needed for enrollment in RTP pricing programs and how this data is managed.
7.3	The data quality principle applies - customers need the ability to review and update this information as residences or businesses change hands and new occupants may want to revise the RTP pricing arrangement if that option is available to them. While the utility is presumed to have the direct relationship with the consumer, there may be intermediated situations where a Third Party Energy Services Provider manages the consumer relationship as a DR or EE aggregator, or manages Direct Load Control (DLC) on behalf of the consumer. The consumer may not be aware of all the entities involved in their participation in RTP pricing programs. The utility should consider clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the “data chain” that may be in place based on their relationships with utility, utility-authorized Third Parties, and/or ESPs that are not affiliated with a utility.

	AICPA Principle	Applies: X	Notes
7.4	**Management Principle**	X	Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
7.5	**Notice Principle**	X	Customers should be given notice for the types of data collected, how it will be used, shared and retained.
7.6	**Choice and Consent Principle**	X	Consumers may be given a choice regarding this pricing option, but it is not a privacy concern if all utility consumers are enrolled in this pricing scenario.
7.7	**Collection Principle**	X	Consumer data is collected as part of any enrollment process in TOU pricing – whether done directly as a pricing switch or as part of a DR program. Provide adequate information about the data that is collected
7.8	**Use and Retention Principle**	X	Any data that is used or retained for analytics purposes should be anonymized and its treatment disclosed to consumers.
7.9	**Access Principle**	X	All consumers have access to their data. Access should be limited to only those with a specific job responsibility requiring such access.
7.10	**Disclosure to Third Parties Principle**	X	Energy Service Providers (ESPs) may have the direct relationship with consumers enrolled in TOU programs and have personal data as well. Consumers should be aware if this principle and all others are equally applicable with any ESP.
7.11	**Security for Privacy Principle**	X	As utilities will house their operations in their own or authorized Contracted Agent facilities, physical and logical security should be in place. If there is equipment that is not under the utility's physical control which contains personal data, physical security will be dependent on the customer or an ESP. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
7.12	**Quality Principle**	X	As is the case for security, quality will be critical for operational purposes.
7.13	**Monitoring and Enforcement Principle**	X	Develop and maintain audit policies to ensure that procedures are consistently applied with regards to personal data.

Category: Demand Response	Privacy Use Case #8
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 with all of the benefits that they can profitably use or manage.

Smart Grid Characteristics	Cybersecurity 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

8.1	**Data Privacy Recommendations** Utilities have personal consumer information such as name, phone number and address for billing. If customer has opted for an electronic payment arrangement, the utility would also have sensitive financial data in cases of payments from consumers. The security safeguard principle has specific application here.
8.2	The use and retention principle applies - utilities should provide notification of why personal data is needed for enrollment in TOU pricing programs and how this data is managed.
8.3	The data quality principle applies - customers need the ability to review and update this information as residences or businesses change hands and new occupants may want to revise the TOU pricing arrangement if that option is available to them.
8.4	While the utility is presumed to have the direct relationship with the consumer, there may be intermediated situations where a Third Party Energy Services Provider manages the consumer relationship as a DR or EE aggregator, or manages Direct Load Control (DLC) on behalf of the consumer. The consumer may not be aware of all the entities involved in their participation in TOU pricing programs. The utility should consider clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the "data chain" that may be in place based on their relationships with utility, utility-authorized Third Parties, and/or ESPs that are not affiliated with a utility.

	AICPA Principle	Applies: X	Notes
8.5	**Management Principle**	X	Establish and maintain policies that oversee the implementation and compliance with the related

			privacy and security policies to protect the data involved with this use case.
8.6	**Notice Principle**	X	Utilities should provide notice to customers participating in TOU pricing programs of the personal data that will be collected related to this activity, and the related purposes for the collection. Information about data access that will or may be given to a Contracted Agent should be provided in the initial notice to the customer. The notice may be listed by service (e.g., data formatting, billing) instead of contractor's company name. Separate notice is not necessary for the sharing of personal data with a Contracted Agent, unless the purpose is materially different than has been previously authorized.
8.7	**Choice and Consent Principle**	X	Consumers may be given a choice regarding this pricing option, but it is not a privacy concern if all utility consumers are enrolled in this same pricing scenario.
8.8	**Collection Principle**	X	Consumer data is collected as part of any enrollment process in TOU pricing – whether done directly as a pricing switch or as part of a DR program. Collect only the data necessary to support the enrollment process and provide adequate information about the data that is collected within the notice.
8.9	**Use and Retention Principle**	X	Any data that is used or retained for TOU, analytics, or other purposes should be anonymized and its treatment disclosed to consumers.
8.10	**Access Principle**	X	All consumers should be provided with a process to have access to their data. Access should be limited to only those with a specific job responsibility requiring such access.
8.11	**Disclosure to Third Parties Principle**	X	Energy Service Providers (ESPs) may have the direct relationship with consumers enrolled in TOU programs and have personal data as well. Consumers should be aware if this principle and all others are equally applicable with any ESP.
8.12	**Security for Privacy Principle**	X	As Utilities will house their operations in their own or authorized Contracted Agent facilities, physical, administrative, and technical security should be in place under their existing information security program. If there is equipment that is not under the utility's physical control that contains personal data, physical, administrative and technical security will be dependent on the customer or an ESP. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.

8.13	**Quality Principle**	X	As is the case for security, quality (data accuracy) will be critical for operational purposes.
8.14	**Monitoring and Enforcement Principle**	X	Access logs for TOU related files should be generated and regular audits of those logs should occur.

Category: Demand Response	Privacy Use Case #9

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 may increasingly be implemented in homes and small businesses, even parking lots.

Smart Grid Characteristics	**Cybersecurity 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

9.1	**Data Privacy Recommendations** Utilities have personal consumer information such as name, phone number and address for billing. If customer has opted for an electronic payment arrangement, the utility would also have sensitive financial data and perhaps authorized access to deposit funds in cases of payments to consumers. The security safeguard principle has specific application here.
9.2	The use and retention principle applies - utilities should provide notification of why personal data is needed for billing and how this data is managed.
9.3	The data quality principle applies - customers need the ability to review and update this information as residences or business change hands and new occupants may want to revise the DR or net metering arrangement.
9.4	While the utility is presumed to have the direct relationship with the consumer, there may be intermediated situations where an Energy Services Provider manages the DR relationship as an aggregator, or manages generation on behalf of the consumer. While the utility is presumed to have the direct relationship with the consumer, there may be intermediated situations where an Energy Services Provider manages generation on behalf of the consumer. The consumer may not be aware of all the entities involved in their participation in a DR program. The utility should consider clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the “data chain” that may be in place based on their relationships with utility, authorized Third Parties, and/or ESPs.

	AICPA Principle	Applies: X	Notes
9.5	**Management Principle**	X	Maintain policies and supporting procedures that govern compliance with the related privacy and security policies to protect the data involved with this use case.
9.6	**Notice Principle**	X	Given that net metering situations will be a result of specific customer choice to enter into the tariff / arrangement, it seems that these two principles will likely be addressed in the process of signing up for net metering.
9.7	**Choice and Consent Principle**	X	
9.8	**Collection Principle**	X	Only the information necessary to support net monitoring for DERs and PEVs should be collected.
9.9	**Use and Retention Principle**	X	Particular emphasis should be placed on this in situations where a Third Party is involved so that consumer data is not misused by that Third Party.
9.10	**Access Principle**	X	Access to the data related to DER and PEV use should be limited to only those with a need for access to support the related business purposes.
9.11	**Disclosure to Third Parties Principle**	X	Energy Service Providers (ESPs) may have the direct relationship with DR or net metering customers and may have personal data as well. Consumers should be aware if this principle and all others are equally applicable with any ESP.
9.12	**Security for Privacy Principle**	X	As utilities will house their operations in their own or authorized Contracted Agent facilities, physical and logical security should be in place. If there is equipment that is not under the utility's physical control which contains personal data, physical security will be dependent on the customer or an ESP. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
9.13	**Quality Principle**	X	As is the case for security, quality (data accuracy and integrity) will be critical for operational purposes.
9.14	**Monitoring and Enforcement Principle**	X	Access logs for TOU related files should be generated and regular audits of those logs should occur.

Category: Demand Response	Privacy Use Case #10
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 (FiT) 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	Cybersecurity 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

10.1	**Data Privacy Recommendations** Utilities have personal consumer information such as name, phone number and address for billing. If customer has opted for an electronic payment arrangement, the utility would also have sensitive financial data and perhaps authorized access to deposit funds in cases of payments to consumers. The security safeguard principle has specific application here.
10.2	The use and retention principle applies - utilities should provide notification of why personal data is needed for billing and how this data is managed.
10.3	The data quality principle applies - customers need the ability to review and update this information as residences or businesses change hands and new occupants may want to revise the DR or net metering arrangement.
10.4	While the utility is presumed to have the direct relationship with the consumer, there may be intermediated situations where an Energy Services Provider manages generation on behalf of the consumer. The consumer may not be aware of all the entities involved in their participation in a FiT program. The utility should consider clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the “data chain” that may be in place based on their relationships with utility, authorized Third Parties, and/or ESPs.

	AICPA Principle	Applies: X	Notes
10.4	Management Principle	X	Responsibility for privacy and information security management must be assigned, and policies and supporting procedures created to apply to the data within this use case. As the only difference here is in the actual pricing of the service, the privacy principles and comments for the net metering for DER and PEV use case 11 apply here. Maintain policies and supporting procedures that govern compliance with the related privacy and security policies to protect the data involved with this use case.
10.5	Notice Principle	X	Customer should be provided with notice of the types of personal data that will be collected as part of the use case. Given that FiT situations will be a result of specific customer choice to enter into the tariff / arrangement, this principle will be best addressed in the process of signing up for an FiT.
10.6	Choice and Consent Principle	X	Given that FiT situations will be a result of specific customer choice to enter into the tariff / arrangement, this principle will be best addressed in the process of signing up for an FiT.
10.7	Collection Principle	X	Only the additional data, beyond that already in possession for energy service, necessary for FiT should be collected.
10.8	Use and Retention Principle	X	As with any type of personal data, FiT data should only be retained as long as possible to support business purposes, and as required by applicable legal requirements. Particular emphasis should be placed on this in situations where a Third Party is involved so that consumer data is not misused by that Third Party.
10.9	Access Principle	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
10.10	Disclosure to Third Parties Principle	X	Energy Service Providers (ESPs) may have the direct relationship with FiT customers and have personal data as well. Consumers should be aware if this principle and all others are equally applicable with any ESP.

10.11	Security for Privacy Principle	X	As utilities will house their operations in their own or authorized Contracted Agent facilities, physical and logical security should be in place. If there is equipment that is not under the utility's physical control which contains personal data, physical security will be dependent on the customer or an ESP. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
10.12	Quality Principle	X	The quality (accuracy) of the personal data used for FiT will be critical for operational purposes. NOTE: Accuracy of personal data is both a privacy and security issue.
10.13	Monitoring and Enforcement Principle	X	Access to FiT data should be logged, and regularly audited, to ensure it is being used appropriately. This helps to address the insider threat that so often causes privacy breaches.

Category: Demand Response	Privacy Use Case #11
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 (CPP) 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	Cybersecurity 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 FiT 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

11.1	**Data Privacy Recommendations** Utilities may have personal consumer data such as name, phone number and address for billing. If customer has opted for an electronic payment arrangement, the utility would also have sensitive financial data and perhaps authorized access to deposit funds in cases of payments to consumers. The security safeguard principle has specific application here.
11.2	The use and retention principle applies - utilities should provide notification of why personal data is needed for billing and how this data is managed.
11.3	The data quality principle applies - customers need the ability to review and update this information as residences or business change hands and new occupants may want to revise the CPP arrangement.
11.4	ESPs or other Contracted Agents who act as utility agents may have access to personal data. The consumer may not be aware of all the entities involved in their participation in a CPP program. The utility should consider clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the “data chain” that may be in place based on their relationships with utility, authorized Contracted Agents, and/or ESPs.

	AICPA Principle	Applies: X	Notes
11.5	Management Principle	X	As the only difference here is in the actual pricing of the service, the privacy principles and comments for the net metering for DER and PEV (Privacy Use Case 12) apply here. Maintain policies and supporting procedures that govern compliance with the related privacy and security policies to protect the data involved with this use case.
11.6	Notice Principle	X	Given that CPP situations will be a result of specific customer choice to enter into the tariff / arrangement, it seems that this principle should be addressed in the process of signing up for CPP.
11.7	Choice and Consent Principle	X	Given that CPP situations will be a result of specific customer choice to enter into the tariff / arrangement, it seems that this principle will likely be addressed in the process of signing up for CPP.
11.8	Collection Principle	X	If additional data is collected to support this use case scenario, it should be limited to only that necessary to support the actions within the scenario.
11.9	Use and Retention Principle	X	Particular emphasis should be placed on this in situations where a Third Party is involved so that consumer data is not misused by that Third Party.
11.10	Access Principle	X	Access should be limited to only those with a specific job responsibility requiring such access.
11.11	Disclosure to Third Parties Principle	X	Energy Service Providers (ESPs) may have the direct relationship with CPP customers and have personal data as well. Consumers should be aware if this principle and all others are equally applicable with any ESP.
11.12	Security for Privacy Principle	X	As utilities will house their operations in their own or authorized Contracted Agent facilities, physical and logical security should be in place. If there is equipment that is not under the utility's physical control which contains personal data, physical security will be dependent on the customer or an ESP. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
11.13	Quality Principle	X	Data needs to be as accurate as possible and applicable for the purposes for which it is used.

11.14	Monitoring and Enforcement Principle	X	Access to pricing data should be logged, and regularly audited, to ensure it is being used appropriately. This helps to address the insider threat (from mistakes, doing things unwittingly, and from malicious intent) that so often causes privacy breaches.

Category: Demand Response	Privacy Use Case #12
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	**Cybersecurity 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

12.1	**Data Privacy Recommendations** This use case presumes residential (one owner/car) situations, but DR may also be used with EV fleets that are common to governmental entities and other businesses. These recommendations address residential situations only. There are three possible grid interfaces considered here: basic 120 V or 240 V plug for electricity downloads connected to a dumb or smart meter; a meter that is capable of running backwards for download and upload of electricity (net metering); and charging stations that can charge/discharge electricity to and from the grid. From the perspective of customer relationship - utilities are involved in the first two interfaces in terms of owning the meter, but the third scenario may involve Third Parties that intermediate the utility/consumer relationship with ownership of charging stations. This would be similar to the situation in which old pay telephones were owned by a number of different vendors, not just the phone company. Consumers may not always be aware of the "ownership" of the charging point and may assume that the privacy policies and practices the utility adopts apply in all scenarios. Utilities may wish to add a statement in their general privacy policies that serves to educate consumers that there are select situations where EV energy consumption data (or other data) could be handled by Third Parties that are not required to abide by utility privacy policies.
12.2	Roaming models for AC charge billing purposes are developing around the world. DC charging appears to be settled into the familiar gas station analogy of credit/debit/cash payments, although affluent customers may opt for similar charging stations. Industry speculation is that credit cards or mobile phones will be the common payment mechanism for roaming AC charging, and may entirely bypass utility operations. However, here are some other scenarios to consider: Utilities may have personal consumer data such as name, credit card/debit card, phone number and address for billing for any roaming charge programs that they manage. In addition, customers may

	have opted for an electronic payment arrangement, so the utility would also have sensitive financial data and perhaps authorized access to deposit funds in cases of payments to consumers. For instance, in California the IOUs are not allowed to provide charging stations, so all charging stations will be owned by Third Party energy service providers, property owners, or businesses. However, these utilities may still have smart charging agreements in place with specific cars or charging stations and will require this information. The security safeguard principle has specific application here. For charging or discharging that occurs away from the consumer's home address but is billed back to a utility account, utilities will need to determine what non-home address location information is necessary to collect for billing/payment purposes, and what should be displayed on paper or electronic bills. Consider the amount of identification that appears on a bank statement if a consumer uses an ATM, or the level of detail on credit card statements for gas purchases to develop policies. Consider the minimum necessary information about charge time, date, and location on electric bills. The purpose specification and accountability principles apply here. Charging Service Providers (CSPs) or other Contracted Agents who act as utility agents may have access to personal data for billing purposes. The consumer may not be aware of all the entities involved when they plug into a charging station. The utility should consider clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the "data chain" that may be in place based on their relationships with utility, authorized Contracted Agents, and/or CSPs. The notice principle applies here. The potential for the collection of location information creates special privacy concerns regarding PEVs. It actually creates special safety and security concerns as well. This is pertinent for charging information that occurs at the consumer's home, not just away from home. This is because PEV charging at home can inform of habits and motoring range for any given date and time. This information is of special interest to law enforcement. Further, it allows individuals to be tracked and stalked, endangering their safety.

	AICPA Principle	**Applies: X**	**Notes**
12.3	Management Principle	X	This use case covers mobile or roaming charge/discharge. At home, charging/discharging information related to PEVs provides motoring range and habit information that can endanger a person's safety and freedom. This requires special privacy protection. When using a Third Party charging station, there is a need to determine how all principles apply, and how consumers are educated is important. It may not be appropriate for a utility to address this issue, but it could still be a smart grid issue. Consumers will appreciate education from a trusted source to understand what personal data may be collected, used, and retained by various entities in mobile charging scenarios. Utilities will need to determine and assign responsibility for how EVs are incorporated into DR programs, and then develop appropriate privacy policies regarding any personal data that would accompany the reporting, billing, and management of these DR programs.

12.4	Notice Principle	X	Notice may be challenging when it is a charging station owned by a Third Party as discussed above in 12.1. Special efforts must be required of Third Parties through the contracts between the Third Parties, utility authorized Contracted Agents, and utilities. Utilities should ensure that authorized Contracted Agents adhere to the privacy policies and practices enacted by the utility to protect PII and energy consumption data. For unrelated Third Parties, utilities lack immediate and/or ongoing opportunities to inform consumers that different privacy policies may be in effect. Utilities may wish to add a statement to their general privacy policies that addresses EV charging devices that are "in their control" or "out of their control." and the consumers must be made aware of the risk of disclosure of this information.
12.5	Choice and Consent Principle	X	There may be choices available at the charging stations/points. If not, then the charging station should clearly indicate the data being collected, how it will be used, shared and retained, and then obtain consent to use the data as a consequence of charging at that location.
12.6	Collection Principle	X	This principle applies for any entity that is delivering power or maintaining a financial transaction. Only the data necessary for the customer to obtain the electricity charge, and then for the charging company to be financially reimbursed, should be collected.
12.7	Use and Retention Principle	X	Data collected from PEV charging stations should be used only for the purposes of supporting the associated payments, and then irreversibly deleted after they are no longer needed for business purposes. If data is intended for planning, balancing, or operational purposes, the utility should adopt Privacy enhancing technologies and practice to anonymize this data and de-identify it.
12.8	Access Principle	X	Since charging stations may be owned by a number of entities, it may be difficult for individuals to know who to contact to gain access to their personal data. PEV charging stations need to ensure customers can get access to their associated PEV charging data, and access to that data within related businesses should be limited to only those with a business need to know.
12.9	Disclosure to Third Parties Principle	X	Since charging stations may be owned by a number of entities, it may be challenging to obtain implicit or explicit consent before sharing data. Even if consent is not feasible, consumers should be told the ways in which the data is used.

12.10	Security for Privacy Principle	X	Applies with special regard to any financial transactions. Applies with special regard to location-based information. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
12.11	Quality Principle	X	PEV charging data must be accurate, and controls need to be incorporated to ensure this.
12.12	Monitoring and Enforcement Principle	X	Develop and maintain audit policies to ensure that procedures are consistently applied with regards to personal data.

Category: Customer Interfaces	Privacy Use Case #13
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 in-home 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	Cybersecurity 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

13.1	Data Privacy Recommendations The information for in-home displays (IHDs) or computers may be richer than the information transmitted by a load control device or communicating thermostat. However, with the possible exception of web portals viewed on computer screens, these devices do not transmit personal data about consumers. The devices are associated with a meter and are simply seen as additional loads to be met in a building. Utility practices regarding personal data handled in billing processes needs to be assessed with regards to new energy consumption data that may be communicated in bills, on IHD devices, on mobile devices, or via computer screens.
13.2	Security practices come into play to protect these devices from unauthorized access – specifically for the communications processes that could transmit control signals to communicating thermostat, load control device, or smart appliance appliances.
13.3	Communications to IHDs need to be considered from a security perspective – are the signals originating from a device in the home – like a WiFi router, and is that router password-protected or not? It is most likely that communications networks for computers and mobile devices have some level of security offered by the communications service provider, but end users should be aware before configuring the device that energy consumption data may be transmitted over these networks and they should avail themselves of all the protections offered by these providers.
13.4	Utilities that collect energy consumption data will need to develop policies for all AICPA principles, and pay particular attention to use and retention. Any use of data by Third Parties will mean that utilities must obtain consent to make that data available to Third Parties.
13.5	Due to the evolution of energy consumption/provision measurement devices into communication devices, special care must be exercised regarding their implementation. They open up the risk of interpretation of communications information laws to apply to energy consumption, and thus increase the risk of inadvertent disclosure through data breaches.

	AICPA Principle	Applies: X	Notes
13.6	**Management Principle**	X	Insofar as programmable communicating thermostats, in home displays, load control and smart appliances that are simply devices "beyond the meter", their energy use is just additional kWh in a utility bill. All principles apply to utility management of personal data in billing processes. This principle is relevant for energy consumption data as a form of personal data. Policies, procedures, and oversight must be established covering these issues. Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
13.7	**Notice Principle**	X	This principle is relevant. Customers need to be provided notice regarding the data being collected, generated, accessed, and how it is used prior to establishing the service.
13.8	**Choice and Consent Principle**	X	Individuals should be provided with an "opt in" or "opt out" choice for utilities to use energy consumption data for any purpose other than billing or other authorized purposes, and for specific features of the devices' services.
13.9	**Collection Principle**	X	Applies to energy consumption data, and utilities should address their interests in analyses of data to deliver better quality of service and/or additional services that will be of value to individuals. Only the data necessary to achieve these services should be collected.
13.10	**Use and Retention Principle**	X	Specific application with regards to energy consumption data and analytics. Utilities should provide a statement that describes why analytics optimize reliability, quality or cost of electricity services. Information should indicate how long the data will be retained, and for what purposes.
13.11	**Access Principle**	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access. Similarly, procedures should be created that will allow customers to have access to the information/data involved with this use case. Utilities may wish to advise customers that Third Parties, unlike Contracted Agents, may not have the same privacy guidelines and practices regarding personal data.
13.12	**Disclosure to Third Parties Principle**	X	Applies, with emphasis on the analyses of energy consumption data – whether anonymized or not.

			Controls need to be applied, using contractual requirements as well as data protection best practices for data sharing (see the NISTIR 7628. Volume 2). Customers should know the entities that have their data.
13.13	**Security for Privacy Principle**	X	Consumers will need assurances that any devices that may be authorized for limited control by utilities, such as setting AC temperatures higher on peak days, are managed via secure communications to prevent unauthorized access by entities inside utilities or external entities. Policies and procedures need to be implemented establishing the safeguards required for the data associated with this use case. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
13.14	**Quality Principle**	X	Insofar as programmable communicating thermostats, in home displays, load control and smart appliances that are simply devices “beyond the meter”, their energy use is just additional kWh in a utility bill. All principles apply to utility management of personal data in billing processes if the provisioning of these devices or their ongoing operation incur fees that appear in utility bills or bills created by Contracted Agents. Procedures need to be followed to ensure data is as accurate as required for the purposes for which it is used.
13.15	**Monitoring and Enforcement Principle**	X	Given sensitivities around privacy and smart meters, strong policies and practices of monitoring and consistent enforcement must be implemented to help allay consumer concerns about energy consumption data.

Category: Customer Interfaces	Privacy Use Case #14
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	**Cybersecurity 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

14.1	**Data Privacy Recommendations** This scenario identifies pricing information or energy data on an In-Home-Device (IHD) via a variety of communication paths. We will discuss two – communications path to a smart meter, and communications path to a Third Party that uses WiFi. We will also consider IHDs to be dedicated, single purpose devices for this scenario, and exclude web portals, tablets, and smart phones. We will also exclude any scenario where electricity is flowing back to the utility, so no net metering information would be displayed on these IHDs.
14.2	In the case where the communications path is from an IHD to a smart meter, the utility should ensure that data that is transmitted to IHDs should not include any personal data – specifically granular energy consumption data - without exercising the choice and consent principle to educate consumers that they consent to display this data.
14.3	In the case where the IHD is receiving information via some other source than a smart meter, it is important to establish where the utility's custody of information such as energy consumption terminates. If an authorized Contracted Agent is reading a meter and communicating that information to an application that wirelessly updates an IHD display, the utility has control over that data because that agent is working in an official capacity with the utility. In these cases, the utility must ensure that all principles, particularly choice and consent, collection, access, notice, use and retention, and disclosure are addressed with consumers.
14.4	IHDs may be selected by consumers independent of utility actions. In this case, utilities have no control over how any data that is extracted from a meter or added by a consumer is displayed. In this case, IHD manufacturers should inform consumers about the types of information that may be collected, retained, and/or displayed.
14.5	Security for privacy principles should come into play to protect IHDs from unauthorized access – specifically for the communications processes that could transmit personal data.

	AICPA Principle	Applies: X	Notes
14.6	**Management Principle**	X	The information that a utility provides to a customer should be based on successful password-protected login to an account. Such practices must be followed and managed using established and consistently applied procedures. Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
14.7	**Notice Principle**	X	This applies for utility and Third Party situations. Customers should be given notice for the types of data collected, how it will be used, shared and retained.
14.8	**Choice and Consent Principle**	X	This is important to educate consumers about what information is displayed in an IHD. Customers should be given choices with regard to the data collected and used to the extent possible for each associated purpose.
14.9	**Collection Principle**	X	This applies for any enrollment process that a utility uses to receive information from an IHD, as well as the actual display of information itself. Only data needed to fulfill the business purposes of this use case should be collected, and no more than necessary.
14.10	**Use and Retention Principle**	X	Since the information is being pushed from a utility smart meter or by a Third Party means to an IHD, the data should be used only for the purposes for which it was collected, and retained only for as long as necessary for those purposes.
14.11	**Access Principle**	X	The ability to view information about a customer account reinforces this principle, but many IHDs may not support this capability. Therefore, procedures need to be established to provide customers access to their associated information. Access to personal data should be limited to only those with a specific job responsibility requiring such access.
14.12	**Disclosure to Third Parties Principle**	X	This applies in scenarios where utilities have selected Third Parties to provision and/or manage deployment of IHDs. Controls need to be applied, using contractual requirements as well as data protection best practices for data sharing (Consider using the DoE Voluntary Code of Conduct or the NAESB REQ.22 standard.). Customers should know the entities that have their data.
14.13	**Security for Privacy Principle**	X	Information transmission security is important. Risk based information security policies and supporting

			procedures should be implemented and consistently followed. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
14.14	**Quality Principle**	X	Procedures and technical controls should be implemented to ensure data stays as accurate as necessary to support the business purposes for which it was collected.
14.15	**Monitoring and Enforcement Principle**	X	Contracted Agents operate under the same privacy guidelines as the utilities that contract them, so utilities have a responsibility to have some sort of processes in place to monitor and enforce their policies on Contracted Agents. Third parties are not necessarily subject to utility privacy policies, so utilities may wish to make note of that in their privacy notice to customers.

Category: Customer Interfaces	Privacy Use Case #15
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	Cybersecurity 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

15.1	**Data Privacy Recommendations** Customer: A communication error on the part of a programmable communicating thermostat, in home display, load control and/or smart appliance may result in a dearth of data, not a display or sharing of personal data if it shows energy usage and/or specific times, dates, appliances, etc. A performance error on the part of a programmable communicating thermostat, in home display, load control and/or smart appliance may cause consumer frustration, but will not necessarily result in a display or sharing of personal data. A loss of power to a programmable communicating thermostat, in home display, load control and/or smart appliance may cause consumer reprogramming, but will not necessarily result in a display or sharing of personal data.
15.2	Device vendor: A communication or performance error on the part of a programmable communicating thermostat, in home display, load control and/or smart appliance will likely result in a support call from either the consumer to the device manufacturer or vice versa. The personal details that may be shared could possibly include consumer name to initiate a support call if the consumer is the caller. If it is a distributor, personal data is unlikely to be shared. A loss of power to a programmable communicating thermostat, in home display, load control and/or smart appliance may cause consumer reprogramming, but will not necessarily result in a display or sharing of personal data. It is unlikely that a support call will be initiated for a power loss. Vendors that take support calls should examine the policies and practices for handling customer data by support operations that typically see or take control (it should be with customer permission) of computer screens to conduct troubleshooting and resolution functions. Similar practices could be enacted that conform to the AICPA principles, particularly with regard to notice, choice and consent, and use and retention.

15.3	Utility: A communication error on the part of a programmable communicating thermostat, in home display, load control and/or smart appliance will likely result in a support call from either the consumer or the entity that sold or provided the device to the consumer or the utility. A performance error on the part of a programmable communicating thermostat, in home display, load control and/or smart appliance may cause consumer frustration, but will not necessarily result in a display or sharing of personal data. In both cases above, if the utility does not provide support for devices, then there is no need to collect any personal data. If the utility offers support or arranges support via an authorized Contracted Agent, any consumer personal data must be safeguarded as outlined by the principles below. A loss of power to a programmable communicating thermostat, in home display, load control and/or smart appliance may trigger a call from the consumer to the utility, but the trouble ticket will be for an outage, not a device malfunction. Utilities that take support calls should have policies and practices that cover handling customer data by support operations that typically see or take control, with customer permission, of computer screens to conduct troubleshooting and resolution functions. Similar practices could be enacted that conform to the AICPA principles particularly with regard to notice, choice and consent, and use and retention. [Outage notifications sent to any display outside the premise should be designed to not include address information to protect consumers from inadvertent displays or announcements of this personal data.]

	AICPA Principle	Applies: X	Notes
15.4	**Management Principle**	X	Policies and supporting procedures need to be established and consistently followed based upon the specific data items involved, as implemented by the utility. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
15.5	**Notice Principle**	X	Notice needs to be given depending upon whether personal data, or data that can reveal personal activities, locations, etc., are involved. Customers should be given notice for the types of data collected, how it will be used, shared and retained.
15.6	**Choice and Consent Principle**	X	Customers need to be given notice for the data involved, why it is necessary and then, as feasible, be given a choice for which data items to provide consent for use.
15.7	**Collection Principle**	X	Only the data necessary for the associated purpose should be collected.
15.8	**Use and Retention Principle**	X	How is data that is personal data, or that can reveal personal activities, or other associated personal data such as appliances, used? The uses should only be for the purposes for which it was collected, and then retained for only the amount of time necessary to fulfill the business reasons for the collection.

15.9	**Access Principle**	X	Procedures should be created to provide customers with access to the data, or to a description of the data, involved with this use case. Access to personal data should be limited to only those with a specific job responsibility requiring such access.
15.10	**Disclosure to Third Parties Principle**	X	This principle should be applied in scenarios where a Third Party or Contracted Agent is are involved in support or troubleshooting. Controls need to be applied, using contractual requirements, where appropriate, as well as data protection best practices for data sharing (see Appendix D: Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties).
15.11	**Security for Privacy Principle**	X	In a troubleshooting scenario, this principle should be taken into account. Security and safeguard controls must be applied as appropriate to mitigate risks and protect personal data and other information that reveals personal activities and characteristics. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
15.12	**Quality Principle**	X	Procedures and technical controls should be implemented to ensure data stays as accurate as necessary to support the business purposes for which it was collected.
15.13	**Monitoring and Enforcement Principle**	X	Utilities should establish policies, procedures, and possibly even a dedicated position, to ensure requirements are monitored and compliance enforced.

Category: Customer Interfaces	Privacy Use Case #16
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	Cybersecurity 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

16.1	**Data Privacy Recommendations** These devices almost certainly contain personal data about consumers that was placed there by consumers. However, utility practices should be designed to not push any personal data to these devices unless a successful login with password has been completed.
16.2	Utility outage notifications pushed to smart phones and computers should not identify personal information on the first screen, but should be designed to offer the consumer an option to receive that additional information.
16.3	Security practices around authorized access need to be in place to ensure that each consumer is only able to access their account information via web portals for computer or smart phone displays. All privacy practices that utilities apply for standard computer-based viewing would apply to the management of the data displayed for consumers.
16.4	Because the evolution of energy consumption/provision measurement devices into communication devices, special care must be exercised regarding their implementation. They open up the risk of interpretation of communications information laws to apply to energy consumption, and thus increase the risk of inadvertent disclosure through data breaches.

	AICPA Principle	Applies: X	Notes
16.5	**Management Principle**	X	Policies and supporting procedures need to be established and consistently followed based upon the specific data items involved, as implemented by the utility. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.

16.6	**Notice Principle**	X	Notice needs to be given depending upon whether personal data, or data that can reveal personal activities, locations, etc., are involved.
16.7	**Choice and Consent Principle**	X	Customers need to be given notice for the data involved, why it is necessary and then, as feasible, be given a choice for which data items to provide consent for use.
16.8	**Collection Principle**	X	Only the data necessary for the associated purpose should be collected.
16.9	**Use and Retention Principle**	X	How is data that is personal data, or that can reveal personal activities, or other associated personal data such as appliances, used? The uses should only be for the purposes for which it was collected, and then retained for only the amount of time necessary to fulfill the business reasons for the collection.
16.10	**Access Principle**	X	Applicability of (and compliance with) the Access principle must be established in the service offering. Procedures should be established to provide customers access to their associated data. Access to others should be given only to those with a specific job responsibility requiring such access.
16.11	**Disclosure to Third Parties Principle**	X	This principle should be applied in scenarios where a Third Party or Contracted Agent is involved in support or troubleshooting. Controls need to be applied, using contractual requirements, where appropriate, as well as data protection best practices for data sharing (see Appendix D: Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties).
16.12	**Security for Privacy Principle**	X	The price paid for electric service may be considered as information impacting personal privacy. Internet access to prices for specific consumers need to be secured appropriately. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
16.13	**Quality Principle**	X	Procedures and technical controls should be implemented to ensure data stays as accurate as necessary to support the business purposes for which it was collected.
16.14	**Monitoring and Enforcement Principle**	X	Utilities should establish policies, procedures, and possibly even a dedicated position, to ensure requirements are monitored and compliance enforced.

Category: Customer Interfaces	Privacy Use Case #17
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	**Cybersecurity 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

17.1	**Data Privacy Recommendations** Utilities would need personal data such as phone number or email address to provide notification, and would need to retain this information for access by outage management systems for automated or manually updated notification. The security safeguard principle has specific application here.
17.2	The purpose specification principle applies - utilities should provide notification of why this data is needed and how this data is managed.
17.3	The data quality principle applies - customers need the ability to review and update this contact information as channel contact preferences may change over time.
17.4	If outage management notification is provided to a contracted Third Party, all utility policies regarding privacy of information apply.
17.5	If outage management notification is provided to a non-contracted Third Party, utilities may wish to provide information to consumers to build awareness about risks to any personally identifiable information delivered by this notification.

	AICPA Principle	**Applies: X**	**Notes**
17.6	**Management Principle**	X	Policies and procedures for providing customer access to update their information, answering their questions, etc. need to exist and periodically be reviewed and updated as necessary to ensure customers' privacy is addressed. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
17.7	**Notice Principle**	X	Must be provided to identify outage management contact purpose. Also to communicate how the data

			will be used. Customers should be given notice for the types of data collected, how it will be used, shared and retained.
17.8	**Choice and Consent Principle**	X	Choice for how to notify. Also to provide consent for the method used to notify, if there are limits on the communication methods.
17.9	**Collection Principle**	X	Collect only the information necessary to allow for these communications.
17.10	**Use and Retention Principle**	X	Retain the communications
17.11	**Access Principle**	X	Customers must have ability to access and update contact data. Access to personal data should be limited to only those with a specific job responsibility requiring such access.
17.12	**Disclosure to Third Parties Principle**	X	May be shared with Third Parties if these are used for outage notification. Customers should be given notice in this case.
17.13	**Security for Privacy Principle**	X	Associated data needs to have appropriate safeguards to ensure minimum access based upon job responsibilities. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
17.14	**Quality Principle**	X	Important to have accurate data, which should be accomplished by providing the customer with access and establishing appropriate procedures and associated technical controls.
17.15	**Monitoring and Enforcement Principle**	X	Important to have accurate data, which should be accomplished by providing the customer with access and establishing appropriate procedures and associated technical controls.

Category: Customer Interfaces	Privacy Use Case #18
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	**Cybersecurity 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

18.1	**Data Privacy Recommendations** Provide secure access according to utility cybersecurity policies to real-time or near real-time energy, demand usage, billing information, pricing information, and utility-supplied applications that control in-home appliances for demand response (DR) purposes.
18.2	Customers may authorize Third Party access to energy use data, and utilities will have to accommodate multiple Third Parties that may be competitors and ensure that practices similar to telecom “slamming” and “cramming” are prevented through strong authorization procedures, particularly based on choice and consent principles.
18.3	For Third Parties, limit the access to only the data needed to accomplish their activities as authorized by utility or customer.
18.4	Protect all pricing information and contact information through use of the principles. To the extent that pricing information is considered personal energy information, it may include payment information for electricity purchased from DER assets owned by customers.
18.5	All recommendations for pre-paid metering (Use case 2) apply to address that energy services scenario above.
18.6	Public EV charging stations have unique challenges in securing any personal data for purposes of payment transactions. If supplied by a utility or the utility has a Third Party contractual relationship with a charging station vendor, ensure that all personal data is handled according to the principles, particularly use and retention and security.

	AICPA Principle	Applies: X	Notes
18.7	**Management Principle**	X	Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
18.8	**Notice Principle**	X	Customers should be given notice for the types of data collected, how it will be used, shared and retained.
18.9	**Choice and Consent Principle**	X	Initial or HAN-related set up of a customer account should include utility statements about any personal data that may be available to utilities or their authorized agents. Account setup or modification should secure customer acceptance of this use of personal data. If Third Party providers may also handle personal data, utilities may wish to consider inclusion of a statement that defines boundaries of utility responsibilities for protecting the privacy of their customers' personal data.
18.10	**Collection Principle**	X	Limit personal data collection to only what is necessary to support these activities.
18.11	**Use and Retention Principle**	X	Retain only as long as the customer is in the program.
18.12	**Access Principle**	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
18.13	**Disclosure to Third Parties Principle**	X	Policies must accommodate multiple Third Parties that may be authorized to access customer data at customer's request.
18.14	**Security for Privacy Principle**	X	Strong safeguards for the data need to be in place. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
18.15	**Quality Principle**	X	Ensure that collected personal data is accurate data, which may be accomplished by providing the customer with access and establishing appropriate procedures to correct any incorrect data.
18.16	**Monitoring and Enforcement Principle**	X	Develop and maintain audit policies to ensure that procedures are consistently applied with regards to customer data

Category: Electricity Market	Privacy Use Case #19
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, previously addressed, 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	**Cybersecurity 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

19.1	**Data Privacy Recommendations** Certain pieces of information must become public information to meet federal regulatory requirements. However, if there is any personal information involved in a transaction that is not required to be disclosed, it should be managed appropriately to preserve privacy.

	AICPA Principle	Applies: X	Notes
19.2	**Management Principle**	X	Entities may include ISO/RTOs or other market clearinghouse agencies. These entities should have someone with assigned responsibility for preserving the privacy of any personal information involved in the transaction that is not required to be disclosed for regulatory purposes.
19.3	**Notice Principle**	X	If there is any personal information involved in a transaction, the customer must be given notice about it. Customers should be given notice for the types of data collected, how it will be used, shared and retained.
19.4	**Choice and Consent Principle**	X	Set up of a customer account as a participant in the bulk electricity market should include utility statements about any personal data that may be available to other organizations or entities. Account setup should secure customer acceptance of this use of personal data.
19.5	**Collection Principle**	X	Limit personal data collection to only what is necessary to support bulk power market activities.

19.6	**Use and Retention Principle**	X	Data on bids may need to be retained for market review.
19.7	**Access Principle**	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
19.8	**Disclosure to Third Parties Principle**	X	Need policies to manage multiple Third Parties that may be authorized to request information about bidders or bids.
19.9	**Security for Privacy Principle**	X	May have heightened importance in competitive generation scenarios. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
19.10	**Quality Principle**	X	Accurate information may be required by regulatory agencies and tax agencies. Ensure that collected personal data is accurate data, which may be accomplished by providing the customer with access and establishing appropriate procedures to correct any incorrect data
19.11	**Monitoring and Enforcement Principle**	X	Develop and maintain audit policies to ensure that procedures are consistently applied with regards to personal data.

Category: Electricity Market	Privacy Use Case #20
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, previously addressed, 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 scenarios.)

Smart Grid Characteristics	**Cybersecurity 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

20.1	**Data Privacy Recommendations** All pricing information must be managed to remain private unless required for disclosure by some governmental or regulatory request, or as consented to or requested by the customer. If there is any personal information involved in a transaction that is not required to be disclosed, it should be managed appropriately to preserve privacy. Utilities may be required by tariffs to allow greater participation by retail customers into the retail energy market. Those tariffs may have requirements for disclosure of information about market participants that could include personal information. Utilities' privacy notice policies should be reviewed to ensure that customers are informed that personal data may be publicly disclosed as required by state or local tariffs.

	AICPA Principle	Applies: X	Notes
20.2	**Management Principle**	X	Entities may include ISO/RTOs or other market clearinghouse agencies. These entities should have someone with assigned responsibility for preserving the privacy of any personal information involved in the transaction that is not required to be disclosed for regulatory purposes.
20.3	**Notice Principle**	X	If there is any personal information involved in a transaction, the customer must be given notice about it. Customers should be given notice for the types of data collected, how it will be used, shared and retained.

20.4	**Choice and Consent Principle**	X	Set up of a customer account as a participant in the bulk electricity market should include utility statements about any personal data that may be available to other organizations or entities. Account setup should secure customer acceptance of this use of personal data.
20.5	**Collection Principle**	X	Limit personal data collection to only what is necessary to support bulk power market activities.
20.6	**Use and Retention Principle**	X	Data on bids may need to be retained for market review.
20.7	**Access Principle**	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
20.8	**Disclosure to Third Parties Principle**	X	Need policies to manage multiple Third Parties that may be authorized to request information about bidders or bids.
20.9	**Security for Privacy Principle**	X	May have heightened importance in competitive generation scenarios. All personal data collected and created during these activities should be appropriately safeguarded to ensure unauthorized access to or use of the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
20.10	**Quality Principle**	X	Accurate information may be required by regulatory agencies and tax agencies. Ensure that collected personal data is accurate data, which may be accomplished by procedural or technical methods.
20.11	**Monitoring and Enforcement Principle**	X	Develop and maintain audit policies to ensure that procedures are consistently applied with regards to personal data.

Category: Electricity Market	Privacy Use Case #21
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, previously addressed, 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	Cybersecurity 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

21.1	**Data Privacy Recommendations** The carbon trading market is extremely nascent. We considered the bulk electricity market to be a use case that has some similarities and modeled our recommendations based on that. All personal information must be managed to remain private, however, personal data may become public information to meet regulatory requirements of federal or state agencies involved in carbon markets. However, if there is any personal data involved in a transaction that is not required to be disclosed, it should be managed appropriately to preserve privacy.

	AICPA Principle	Applies: X	Notes
21.2	**Management Principle**	X	Entities may include ISO/RTOs or other market clearinghouse agencies. These entities should have someone with assigned responsibility for preserving the privacy of any personal information involved in the transaction that is not required to be disclosed for regulatory purposes.
21.3	**Notice Principle**	X	If there is any personal information involved in a transaction, the customer must be given notice about it.
21.4	**Choice and Consent Principle**	X	Set up of a customer account as a participant in the bulk electricity market should include utility statements about any personal data that may be available to other organizations or entities. Account setup should secure customer acceptance of this use of personal data.
21.5	**Collection Principle**	X	Limit personal data collection to only what is necessary to support bulk power market activities.

21.6	**Use and Retention Principle**	X	Data on bids may need to be retained for market review.
21.7	**Access Principle**	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
21.8	**Disclosure to Third Parties Principle**	X	Need policies to manage multiple Third Parties that may be authorized to request information about bidders or bids.
21.9	**Security for Privacy Principle**	X	May have heightened importance in competitive generation scenarios.
21.10	**Quality Principle**	X	Accurate information may be required by regulatory agencies and tax agencies.
21.11	**Monitoring and Enforcement Principle**	X	Develop and maintain audit policies to ensure that procedures are consistently applied with regards to personal data.

Category: Distribution Automation (DA)	Privacy Use Case #22

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	**Cybersecurity 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 • Cybersecurity

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Distribution Automation	Privacy Use Case #23
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	**Cybersecurity 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

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Distribution Automation	Privacy Use Case #24

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	**Cybersecurity 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

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Distribution Automation	Privacy Use Case #25
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	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity of outage information is critical • Availability to detect large-scale outages usually involve multiple sources of information • Confidentiality is not very important	• Customer safety • Customer device standards • Demand response acceptance by customers

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Distribution Automation	Privacy Use Case #26
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	**Cybersecurity 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

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Distribution Automation	Privacy Use Case #27
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	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity is critical to operate the distribution power system reliably, efficiently, and safely • Availability is critical to operate the distribution power system reliably, efficiently, and safely • Confidentiality is not important	• Customer safety • Customer device standards • Demand response acceptance by customers

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Distribution Automation	Privacy Use Case #28
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	Cybersecurity Objectives/Requirements	Potential Stakeholder Issues
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity is critical for any management/ control of generation and storage • Availability requirements may vary depending on the size (individual or aggregate) of the DER plant • Confidentiality may involve some privacy issues with customer-owned DER	• Customer safety • Customer device standards • Demand response acceptance by customers

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Distribution Automation	Privacy Use Case #29

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	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity not critical due to multiple sources of data • Availability is not important • Confidentiality is not important	• Cybersecurity

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Plug In Hybrid Electric Vehicles (PHEV)	Privacy Use Case #30
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	**Cybersecurity 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

30.1	**Data Privacy Recommendations** Provide secure access to customer billing and related account information during payments at public location.
30.2	Allow only those authorized individuals, with a business need, access to the information within customer accounts related to PHEV charging and discharging information.
30.3	Utility policy for tracking EV charges should determine if date/time/location/duration of charging will be presented as part of bill. This may be particularly relevant to "roaming" charges. Many consumers may appreciate this detail, similar to a credit card monthly statement showing date/ time/location of fueling stops for gas-fueled vehicles. All this data, whether displayed in a bill presentment (printed or online) or not must be protected.
30.4	Fees for charging and payments for discharging are financially sensitive data and should be protected by utility policies already established for this type of information.

	AICPA Principle	**Applies: X**	**Notes**
30.5	**Management Principle**	X	Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.

30.6	**Notice Principle**	X	Policies and procedures to give notice whenever a Third Party requests, or obtain access to, PHEV charging information. This may arise in the case of EV fleet vehicles, which may be assigned to employees who are responsible for charging, but the EV is actually owned by the employer.
30.7	**Choice and Consent Principle**	X	Policies and procedures to obtain consent from customer to give Third Parties access to PHEV data. As noted above, EV driver (customer) and EV owner may be different in select situations. Review utility policies regarding landlords (owners) and tenants (customers) to structure consistent application of practices for what is essentially a rolling, not stationary, specialized charging and discharging asset.
30.8	**Collection Principle**	X	Limit personal data collection to only what is necessary to support business activities.
30.9	**Use and Retention Principle**	X	Policies and procedures to retain customer identifiable data only while the customer is participating in the program.
30.10	**Access Principle**	X	Access to personal data should be limited to only those with a specific job responsibility requiring such access.
30.11	**Disclosure to Third Parties Principle**	X	Policies and procedures for disclosing PHEV charging information access to Third Parties. See discussion about EV drivers as customers and EV owners as Third Parties.
30.12	**Security for Privacy Principle**	X	All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
30.13	**Quality Principle**	X	Ensure that collected personal data is accurate data, which may be accomplished by providing the customer with access and establishing appropriate procedures to correct any incorrect data.
30.14	**Monitoring and Enforcement Principle**	X	Develop and maintain audit and sanction policies to ensure that procedures are consistently applied with regards to personal data.

Category: Plug In Hybrid Electric Vehicles	Privacy Use Case #31
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

31.1	**Data Privacy Recommendations** Safeguard customer information related to the PHEVs, energy usage and billing rates.
31.2	Customers should be able to authorize Third Party access to the PHEV charging program data.

	AICPA Principle	Applies: X	Notes
31.3	**Management Principle**	X	Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
31.4	**Notice Principle**	X	Policies and procedures to give notice to customers for how PHEV program data is used and shared. This may arise in the case of EV fleet vehicles, which may be assigned to employees who are responsible for charging, but the EV is actually owned by the employer.
31.5	**Choice and Consent Principle**	X	Policies and procedures to obtain consent prior to allowing access to additional Third Parties. As noted above, EV driver (customer) and EV owner

			may be different in select situations. Review utility policies regarding landlords (owners) and tenants (customers) to structure consistent application of practices for what is essentially a rolling, not stationary, specialized charging and discharging asset.
31.6	**Collection Principle**	X	Limit personal data collection to only what is necessary to support business activities.
31.7	**Use and Retention Principle**	X	Policies and procedures to retain customer identifiable data only while the customer is participating in the program.
31.8	**Access Principle**	X	Policies/procedures should be in place to allow customers access to their PHEV program account data. Access to personal data should be limited to only those with a specific job responsibility requiring such access.
31.9	**Disclosure to Third Parties Principle**	X	Policies must accommodate multiple Third Parties that may be authorized to access customer data at customer's request.
31.10	**Security for Privacy Principle**	X	All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to or use of the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
31.11	**Quality Principle**	X	Ensure that collected personal data is accurate data, which may be accomplished by procedural or technical methods.
31.12	**Monitoring and Enforcement Principle**	X	Develop and maintain audit and sanctions policies to ensure that procedures are consistently applied with regards to personal data.

Category: Plug In Hybrid Electric Vehicles	Privacy Use Case #32
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 • 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	• Improved system stability and availability • To keep customer information private • To insure DR messages are accurate and trustworthy	• Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

32.1	**Data Privacy Recommendations** Safeguard customer information related to the PHEVs, energy usage, distributed energy provision, and billing and discharging rates.
32.2	Customers should be able to authorize Third Party access to the PHEV charging and provisioning program data.
32.3	Consider vehicle discharging as grid stabilization activity, which presumes a financial transaction between vehicle owner and utility or an aggregator of EVs and a utility. All customer information required for these transactions must be protected.

	AICPA Principle	Applies: X	Notes
32.4	**Management Principle**	X	Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
32.5	**Notice Principle**	X	Policies and procedures to give notice to customers for how PHEV program and provisioning data is used and shared.

32.6	**Choice and Consent Principle**	X	Policies and procedures to obtain consent prior to allowing access to additional Third Parties.
32.7	**Collection Principle**	X	Limit personal data collection to only what is necessary to support business activities.
32.8	**Use and Retention Principle**	X	Policies and procedures to retain customer identifiable data only while the customer is participating in the program.
32.9	**Access Principle**	X	Policies/procedures should be in place to allow customers access to their PHEV program account data. Access to personal data should be limited to only those with a specific job responsibility requiring such access.
32.10	**Disclosure to Third Parties Principle**	X	Policies must accommodate multiple Third Parties that may be authorized to access customer data at customer's request.
32.11	**Security for Privacy Principle**	X	All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to or use of the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
32.12	**Quality Principle**	X	Ensure that collected personal data is accurate data, which may be accomplished by procedural or technical methods.
32.13	**Monitoring and Enforcement Principle**	X	Develop and maintain audit and sanctions policies to ensure that procedures are consistently applied with regards to personal data.

Category: Plug In Hybrid Electric Vehicles	Privacy Use Case #33
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 • 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	• Improved system stability and availability • Pricing signals are accurate and trustworthy • Customer information is kept private	• Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

33.1	**Data Privacy Recommendations** Safeguard customer information related to the PHEVs, energy usage, pricing data, and billing and discharging rates.
33.2	Customers should be able to authorize Third Party access to the PHEV pricing data.
33.3	Consider vehicle discharging as grid stabilization activity, which presumes a financial transaction between vehicle owner and utility or an aggregator of EVs and a utility. All customer information required for these transactions must be protected.

	AICPA Principle	Applies: X	Notes
33.4	**Management Principle**	X	Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed.
33.5	**Notice Principle**	X	Policies and procedures to give notice to customers for how PHEV program and pricing data is used and shared.

33.6	**Choice and Consent Principle**	X	Policies and procedures to obtain consent prior to allowing access to additional Third Parties.
33.7	**Collection Principle**	X	Limit personal data collection to only what is necessary to support business activities.
33.8	**Use and Retention Principle**	X	Policies and procedures to retain customer identifiable data and related pricing data only while the customer is participating in the program.
33.9	**Access Principle**	X	Policies/procedures should be in place to allow customers access to their PHEV pricing program account data. Access to personal data should be limited to only those with a specific job responsibility requiring such access.
33.10	**Disclosure to Third Parties Principle**	X	Policies must accommodate multiple Third Parties that may be authorized to access customer data at customer's request.
33.11	**Security for Privacy Principle**	X	All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to or use of the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
33.12	**Quality Principle**	X	Ensure that collected personal data is accurate data, which may be accomplished by procedural or technical methods.
33.13	**Monitoring and Enforcement Principle**	X	Develop and maintain audit and sanctions policies to ensure that procedures are consistently applied with regards to personal data.

Category: Distributed Resources	Privacy Use Case #34
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	Cybersecurity 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

34.1	**Data Privacy Recommendations** This use case is similar to Use Case 9 (Net Metering of DER and PEV)
34.2	Utilities have personal consumer information such as name, phone number and address for billing. If customer has opted for any payment arrangement to sell electricity back to the utility, the utility would also have sensitive financial data and perhaps authorized access to deposit funds in cases of payments to consumers. The security safeguard principle has specific application here.
34.3	The use and retention principle applies - utilities should provide notification of why personal data is needed for billing and/or payments, and how this data is managed.
34.4	The data quality principle applies - customers need the ability to review and update this information as residences or business change hands and new occupants may want to revise a DER arrangement made on assets that are affixed to property.
34.5	While the utility is presumed to have the direct relationship with the consumer, there may be intermediated situations where an Energy Services Provider (ESP) manages the DER asset on behalf of the consumer. The utility should consider clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the "data chain" that may be in place based on their relationships with utility, authorized Third Parties, and/or ESPs.

	AICPA Principle	Applies: X	Notes
34.6	**Management Principle**	X	Maintain policies and supporting procedures that govern compliance with the related privacy and security policies to protect the data involved with this use case.

34.7	**Notice Principle**	X	Account setups for DER scenarios should include information that describes any personal data that is collected and how it is used, shared and retained.
34.8	**Choice and Consent Principle**	X	Account setup procedures should provide customers with the ability to consent to the described uses of their personal data.
34.9	**Collection Principle**	X	Only the data necessary to support DER accounts should be collected.
34.10	**Use and Retention Principle**	X	Particular emphasis should be placed on this in situations where a Third Party is involved so that consumer data is not misused by that Third Party.
34.11	**Access Principle**	X	Access to the data related to DER use should be limited to only those with a need for access to support the related business purposes.
34.12	**Disclosure to Third Parties Principle**	X	ESPs may have the direct relationship with DER customers and have personal data as well. Consumers should be aware if this principle and all others are equally applicable with any ESP.
34.13	**Security for Privacy Principle**	X	If there is equipment that is not under the utility's physical control which contains personal data, physical security will be dependent on the customer or an ESP. All personal data collected and created during these activities should be appropriately safeguarded to ensure unauthorized access to or use of the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
34.14	**Quality Principle**	X	As is the case for security, quality will be critical for operational purposes. Ensure that collected personal data is accurate data, which may be accomplished by procedural or technical methods.
34.15	**Monitoring and Enforcement Principle**	X	Access to personal data should be logged, and regularly audited, to ensure it is being used appropriately.

Category: Distributed Resources	Privacy Use Case 35
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	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently	• Commands are trustworthy and accurate • Customer's data is kept private • DR messages are received timely	• Safety • Customer data privacy and security

35.1	**Data Privacy Recommendations** This use case is similar to Use Cases 9 and 34.
35.2	Utilities have personal consumer information such as name, phone number and address for billing. If customer has opted for any payment arrangement with the utility, the utility would also have sensitive financial data and perhaps authorized access to deposit funds in cases of payments to consumers. The security safeguard principle has specific application here.
35.3	The use and retention principle applies - utilities should provide notification of why personal data is needed for billing and/or payments, and how this data is managed.
35.4	The data quality principle applies - customers need the ability to review and update this information as residences or businesses change hands and new occupants may want to revise the DER arrangement.
35.5	While the utility is presumed to have the direct relationship with the consumer, there may be intermediated situations where an Energy Services Provider (ESP) manages the DER asset on behalf of the utility (or the customer). The utility should consider clear, simple identification of all entities or some formal statement of the data management principle to help educate consumers as to the "data chain" that may be in place based on their relationships with utility, authorized Third Parties, and/or ESPs.

	AICPA Principle	**Applies: X**	**Notes**
35.6	Management Principle	X	Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are

			effectively communicated to all personnel, and are followed.
35.7	Notice Principle	X	Customers should be given notice for the types of data collected, how it will be used, shared and retained.
35.8	Choice and Consent Principle	X	Since utilities or their agents are given control of a DER asset by the customer, choice and consent write-ups should be clearly and concisely written to identify options for opt outs and opt ins.
35.9	Collection Principle	X	Only the data necessary to support DER accounts should be collected.
35.10	Use and Retention Principle	X	Particular emphasis should be placed on this in situations where a Third Party is involved so that consumer data is not misused by that Third Party.
35.11	Access Principle	X	Access to the data related to DER use should be limited to only those with a need for access to support the related business purposes.
35.12	Disclosure to Third Parties Principle	X	Energy Service Providers (ESPs) may have the direct relationship with DER customers and have personal data as well. Consumers should be aware if this principle and all others are equally applicable with any ESP.
35.13	Security for Privacy Principle	X	As utilities will house their operations in their own or authorized Contracted Agent facilities, physical and logical security should be in place. If there is equipment that is not under the utility's physical control which contains personal data, physical security will be dependent on the customer or an ESP. All personal data collected and created during these activities should be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
35.14	Quality Principle	X	As is the case for security, quality will be critical for operational purposes. Ensure that collected personal data is accurate data, which may be accomplished by providing the customer with access and establishing appropriate procedures to correct any incorrect data.
35.15	Monitoring and Enforcement Principle	X	Develop and maintain audit policies to ensure that procedures are consistently applied with regards to personal data.

Category: Transmission Operations	Privacy Use Case #36

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	Cybersecurity 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

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Transmission Operations	Privacy Use Case #37
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	**Cybersecurity 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	• Cybersecurity

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Transmission Operations	Privacy Use Case #38

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 perform system restorations based on system restoration plans prepared (authorized) by operation management

Smart Grid Characteristics	**Cybersecurity 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

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: Transmission Operations	Privacy Use Case #39
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 synchro-phasor system provides synchronized and time-tagged voltage and current phasor measurements to any protection, control, or monitoring function that requires measurements taken from several locations, whose phase angles are measured against a common, system-wide reference. Present day implementation of many protection, control, or monitoring functions 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	**Cybersecurity 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	• Cybersecurity • Customer data privacy and security

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

Category: RTO/ISO Operations	Privacy Use Case #40
Scenario: RTO/ISO Management of Central and DER Generators and Storage	
Category Description An ISO/RTO control center that participates in the market and does not operate the market.	
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	**Cybersecurity 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 operator commands (e.g. one second) • Confidentiality is not important	• Cybersecurity • Customer data privacy and security

40.1	**Data Privacy Recommendations** If an RTO/ISO has personal customer data associated with a DER asset, these entities would need to exercise the same security and privacy policies that utilities would follow as outlined in Use Case 28 (Distributed Energy Resources Management). However, if only aggregate and not individual data is available to RTO/ISOs, utilities or Third Parties, no privacy impacts would be applicable.
40.2	Analytics applications may be used to assess performance of various programs that engage customer DER assets. These programs may be managed by utilities, RTO/ISOs, or by Contracted Agents or authorized (by utility, RTO/ISO, or customer) Third Parties. • Utilities should exercise their existing policies and practices for personal data when managing DER assets on behalf of customers. To the extent that customers may directly share personal data with Third Parties, the data is then outside of the control of the utilities. • It will be important to ensure through ongoing audits that the Contracted Agents comply with all utility policies regarding any customer data for both privacy and security reasons. • If the Third Party arrangement is between the customer (DER asset owner) and RTO/ISO, the RTO/ISO should emphasize that any consumer data that is shared directly by the consumer with that Third Party is outside of the control of the RTO/ISO.

	AICPA Principle	**Applies: X**	**Notes**
40.3	Management Principle	X	Policies and procedures for providing customer access to update their information, answering their questions, etc. should exist and be updated as

			appropriate whenever business and/or technology changes occur. Particularly for: 1) Direct monitoring and control of DER; 2) Shut-down or islanding verification for DER; and 3) Electric storage fill/draw management.
40.4	Notice Principle	X	Customers should be given notice for the types of data collected, how it will be used, shared and retained.
40.5	Choice and Consent Principle	X	Choice for how to notify. Also to provide consent for the method used to notify, if there are limits on the communication methods.
40.6	Collection Principle	X	Collect only the information necessary to allow for these communications.
40.7	Use and Retention Principle	X	Retain the data and associated communications only as long as necessary, and use the data only for the purposes for which it was collected.
40.8	Access Principle	X	Procedures should be established to allow customers to access and correct appropriate data.
40.9	Disclosure to Third Parties Principle	X	Customers should be given notice in cases where Third Parties have access to personal data, and understand the differences in how data may be handled by RTO/ISO-contracted Third Parties or by independent Third Parties.
40.10	Security for Privacy Principle	X	Associated data needs to have appropriate safeguards to ensure minimum access based upon job responsibilities, and also to protect against other types of unauthorized access. All personal data collected and created during these activities should be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.
40.11	Quality Principle	X	Ensure that collected personal data is accurate data, which may be accomplished by providing the customer with access and establishing appropriate procedures to correct any incorrect data.
40.12	Monitoring and Enforcement Principle	X	Applies for all types of entities (business or individual) that own assets that are connected as DER assets that can transact sale of electricity to RTO/ISOs.

Category: Asset Management	Privacy Use Case #41
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 utility's 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	**Cybersecurity 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 (confidentiality)	• Customer data privacy and security • Cybersecurity

41.1	**Data Privacy Recommendations** The potential exists for abuse of privacy of individual consumer data collected by field devices including event recorders, if, for example the event recorder was associated with an individual meter. This may be a situation that occurs in rural areas where one residential customer may be on a transformer or circuit; for agricultural operations; or for some C&I customers that have dedicated transformers or circuits. However, in general, this is not more or less than the same potential that exists regarding normal equipment that is used to deliver power and perform other functions such as billing. Possibly data stored locally in consumer's on-site equipment that is not available online could pose an additional threat. However, it is not clear that this is the case.
41.2	Generally, the collection of aggregate load data does not seem to pose a privacy risk to individual consumers. Thus, in general, this use case pertains less to the point that field equipment may be used than to the fact that load data is aggregated. From this point of view, AICPA principles would not seem to apply.
41.3	From the point of view of tools and activities related to assessing and maintaining equipment assets, again the privacy threat seems no more or less than that posed by normal energy delivery and data collection activities, again, such as billing.
41.4	The monitoring, collection and storage of information regarding equipment, networks or any other component of the technical service delivery environment would affect consumer privacy to no greater or lesser extent than applies to other data collected.

41.5	However, as noted above, if a transformer or circuit is associated with a single customer, the data collected here would have privacy impacts as there is no aggregation to be had. In these cases of single customer association to a transformer or circuit, privacy policies that govern meter data collection should be followed (Use Case 1).

	AICPA Principle	**Applies: X**	**Notes**
41.6	Management Principle	X	For aggregate load data, this recommendation would not apply**.** For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.
41.7	Notice Principle	X	For aggregate load data, this recommendation would not apply**.** For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.
41.8	Choice and Consent Principle	X	For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.
41.9	Collection Principle	X	For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.
41.10	Use and Retention Principle	X	For aggregate load data, this recommendation would not apply**.** For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.
41.11	Access Principle	X	For aggregate load data, this recommendation would not apply**.** For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.
41.12	Disclosure to Third Parties Principle	X	For aggregate load data, this recommendation would not apply**.** For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.
41.13	Security for Privacy Principle	X	For aggregate load data, this recommendation would not apply**.** For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability.

41.14	Quality Principle	X	For aggregate load data, this recommendation would not apply**.** For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.
41.15	Monitoring and Enforcement Principle	X	For aggregate load data, this recommendation would not apply**.** For monitored equipment that is associated with a single customer, follow the recommendations for Use Case 1 to ensure data privacy.

Category: Asset Management	Privacy Use Case #42

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	Cybersecurity 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	• Cybersecurity • Customer data privacy and security

42.1	**Data Privacy Recommendations** Most scenarios would adhere to the recommendations outlined in Use Case 43. However, the same exceptions apply as noted in that use case. If an asset is associated with a single customer, the data collected here would have privacy impacts as there is no aggregation to be had. In these cases of single customer association to an asset, privacy policies that govern meter data collection should be followed (Use Case 1). Please follow the recommendations for the AICPA principles outlined in Use Case 1 when equipment is associated with a single customer.

Category: Asset Management	Privacy Use Case #43
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	Cybersecurity 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 • Demand Response (DR) messages are received and processed timely	• Demand response acceptance by customers • Customer data privacy and security • Retail Electric Supplier access • Customer data access

43.1	**Data Privacy Recommendations** Overall the recommendations are similar to those for Use Case #42. However, DR programs are associated with individual customers. There could be other load reduction programs such as AC or pool pump cycling that also apply to specific customers. Therefore, personal data including energy data consumption needs protection as outlined in these recommendations for DR programs.
43.2	Demand Response behaviors are customer-specific and participation in these programs may be directly managed by a utility; by a Contracted Agent on behalf of the utility; or by a DR aggregator (Third Party) acting independently from a utility.
43.3	DR participation typically involves a financial transaction, so accuracy of meter read data is extremely important.
43.4	Meter read data is protected information regardless of type of DR program, or if the participant is working with a utility, a Contracted Agent of a utility, or a DR aggregator not affiliated with a utility. Similarly, choice and consent information requires that any DR participant has been notified and consented to Third Party access to the data identified as necessary for that activity.
43.5	Meter reading for DR is an ongoing activity, so it is important that utilities create a monitoring and enforcement process that ensures compliance with privacy protections on an ongoing basis.

43.6	Contracted Agents may be given access to meter reading data for DR program purposes. These agents should also conform and comply with utility privacy policies, and customers must be notified about the disclosure of their information to these Contracted Agents. Notification may occur when the customer enters into a contract with a utility.

	AICPA Principle	Applies: X	Notes
43.7	**Management Principle**	X	Policies and procedures should exist for the data collected, used, shared and stored. A position should exist with assigned accountability for ensuring such policies and procedures exist, are effectively communicated to all personnel, and are followed**.** For aggregate load data, this recommendation would not apply**.**
43.8	**Notice Principle**	X	Would have to be provided for all meter reading in DR scenarios. Customers should be given notice for the types of data collected, how it will be used, shared and retained. For aggregate load data, this recommendation would not apply.
43.9	**Choice and Consent Principle**	X	Ensure that when customers sign up for DR service that this choice and consent requirement is met.
43.10	**Collection Principle**	X	Data collection may change as new applications, technologies, or programs are made available. Utility policy should indicate that collection purposes may change over time and that utilities will notify customers of any proposed changes that may impact collection in order to secure an updated choice and consent.
43.11	**Use and Retention Principle**	X	Retention may be impacted by time frames to record and compensate for DR scenarios. For aggregate load data, this recommendation would not apply.
43.12	**Access Principle**	X	For aggregate load data, this recommendation would not apply.
43.13	**Disclosure to Third Parties Principle**	X	DR payments to customers may be considered revenue or income and thus subject to tax laws, or garnishments for child support, legal claims, etc. Some of the legal implications may not require implicit or explicit consent. For aggregate load data, this recommendation would not apply.
43.14	**Security for Privacy Principle**	X	All personal data collected and created during these

			activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability. For aggregate load data, this recommendation would not apply**.**
43.15	**Quality Principle**	X	Data quality is important for DR program participation. Ensure that collected personal data is accurate data, which may be accomplished by providing the customer with access and establishing appropriate procedures to correct any incorrect data. For aggregate load data, this recommendation would not apply.
43.16	**Monitoring and Enforcement Principle**	X	DR participation may be an ongoing activity. Utilities should create a practice of regular monitoring and provide audits of Contracted Agents. Utilities should also advise that customers may have authorized DR aggregators to have access to meter data. Policy guidance should be defined for where utility responsibility for meter data ends and what rights customers have regarding their data once they have given authorization for a Third Party to access that info. For aggregate load data, this recommendation would not apply.

Category: Asset Management	Privacy Use Case #44
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	• Cybersecurity • Customer data privacy and security

44.1	**Data Privacy Recommendations** Many aspects of this use case are the same as Use case #43. If notification is given to customers about pending corrective actions, utility practices regarding protection of personal data should be exercised.
44.2	Utility resources will consider critical needs flags for residential, commercial, or industrial customers such as home health equipment that requires electricity, health care facilities, etc in determining corrective actions for pending asset failures. Certain customers may be the last to lose electricity as part of any corrective action, or others may be identified as first for restoration of services because of their special circumstances. Utilities already have life-safety policies in place for planned and unplanned outage recovery. These policies should be reviewed to identify any exposure of Personally Identifiable Information. Except as necessary to implement the life-safety policy to preserve the health of the customer, personal data should be removed from records.
44.3	Utility resources will also need to know if there are any customer assets that produce or store energy for two purposes: a) for inclusion in outage recovery plans, and b) for worker safety. Again, information should be limited to identification of asset at customer address and enabled connections to the distribution grid, but limit exposure of personal data.

	AICPA Principle	Applies: X	Notes
44.4	**Management Principle**	X	Customer records may include information about life-safety that may be accessed by utility resources in this scenario. Utility resources will need to be trained to comply with all data privacy policies, and existing utility policies regarding policies for corrective actions must be reviewed for compliance with data privacy policies. For aggregate load data, this recommendation would not apply**.**
44.5	**Notice Principle**	X	When corrective action is about to be taken, the utility would be required to give notice. However, this does not trigger specific privacy or security issues. Utilities should provide an explanation regarding need to know about life-safety situations that require constant electricity for equipment. For aggregate load data, this recommendation would not apply.
44.6	**Choice and Consent Principle**	X	Utilities should indicate that customers who do not provide consent to collection of information regarding healthcare needs may not receive any special consideration in outage and restoration scheduling.
44.7	**Collection Principle**	X	Utilities should indicate to customers that collection of information regarding healthcare needs is necessary for planned and unplanned outage restoration plans.
44.8	**Use and Retention Principle**	X	For aggregate load data, this recommendation would not apply.
44.9	**Access Principle**	X	For aggregate load data, this recommendation would not apply.
44.10	**Disclosure to Third Parties Principle**	X	If Third Parties are involved in outage or restoration services, care must be taken that personal data is not disclosed. For aggregate load data, this recommendation would not apply.

44.11	**Security for Privacy Principle**	X	Since information about health may be involved, this principle must be emphasized in all processes. All personal data collected and created during these activities must be appropriately safeguarded to ensure unauthorized access to the data does not occur, to preserve integrity of the data, and to allow for appropriate availability. For aggregate load data, this recommendation would not apply.
44.12	**Quality Principle**	X	Customers move, conditions change, so any flags about health conditions must be tied to the customer, not to the meter. Ensure that collected personal data is accurate data, which may be accomplished by providing the customer with access and establishing appropriate procedures to correct any incorrect data. For aggregate load data, this recommendation would not apply.
44.13	**Monitoring and Enforcement Principle**	X	For aggregate load data, this recommendation would not apply.

APPENDIX F: SUMMARY OF THE SMART GRID HIGH-LEVEL CONSUMER-TO-UTILITY PRIVACY IMPACT ASSESSMENT

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 (draft v3.0)*[157] in relation to the privacy principles used as the basis for the PIA. Each 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.

   Privacy Practices Recommendations:

   - **Assign privacy responsibility**. Each organization collecting or using smart grid data from or about consumer locations should assign responsibility to a position or person 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 with the customer 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

[157] R. Herold, C. Veltsos, and W. Pyles, *NIST Smart Grid High Level Consumer-to-Utility Privacy Impact Assessment DRAFT v3.0*, September 9, 2009, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/NIST_High_Level_PIA_Report_-_Herold_09_09_09_w-edits.doc [accessed 8/11/2014].

be more transparent and clearly provide notice to the customer 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 and what it will be used for.

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 consumer.

Findings:

In the current operation of the electric utilities, data taken from traditional meters consists of basic data usage readings required to create bills. In the future, smart meters may be enabled to collect other types of data.[158] 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 the provision of electric service to the customer and 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 consumer.

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 and determine energy use trends. The smart grid will provide data that allows customers to take greater control of their usage or consumption by enabling them to make more informed decisions and actions..

   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.

[158] For more discussion on smart meter collection capabilities, see §5.3.1.

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. 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 and theft, and from 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 and theft, and from 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 are responsible for adopting 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, 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, etc.) 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.[159]

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 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.

[159] 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.

APPENDIX G: 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 volume to create a common base of understanding for their use. The energy-specific terms are defined within Appendix J. The following definitions of the terms related to privacy as they are used within this volume.

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, may be 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.

Contracted Agent

An entity under contract with the Third Party to perform services or provide products using CEUD. In some industries, Contracted Agents are referred to as Business Partners or Business Associates.

Customer

Any entity that takes electric service for its own consumption.

Customer/Consumer[160] Energy Usage Data (CEUD)

Energy usage information and data identifiable to a premise or an individual customer obtained without the involvement of the utility.

Individual

Any specific person.

Personal Information

"Personal information" is a broad term that includes personally identifiable information (PII) and 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

[160] There may be a legal issue in terms of who has access to this data. There may be situations in which the Customer and the consumer are not the same and that one might want to restrict access to the CEUD. These recommended practices are not designed to determine legal issues.

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 might 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; or 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 could potentially become a privacy issue in a university, office setting, healthcare facility, and so on.

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 (HIPAA) of 1996 requires the following types of protected health information[161] 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

[161] Per the current (with Omnibus Final Rule provisions implemented) HIPAA requirements located at 45 CFR § 164.514 (b), these specific items must all be removed to be considered as de-identified; and no longer considered to be protected health information. See the full text in U.S. Department of Health and Human Services, Office for Civil Rights, *HIPAA Administrative Simplification*, March 2013, http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf [accessed 8/11/2014].

- 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 genetic information that is unique to an individual;
- Any other unique identifying number, characteristic, or code.

With the exception of those terms specifically naming energy, the above are the items defined within HIPAA, which arguably has the widest definition of PII within the existing U.S. federal regulations. More identifiers may be considered to be PII as the smart grid evolves and as regulations change.

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.

Privacy Use Case

A method of looking at data flows that will help Third Parties to rigorously track data flows and the privacy implications of collecting and using data, and will help the organization to address

and mitigate the associated privacy risks within common technical design and business practices. Use cases can help smart grid architects and engineers build privacy protections into the smart grid.

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 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.

Private information 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 to know. Other individuals, however, communicate how they voted on campaign buttons or t-shirts 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.

Third Party

An entity — other than the electric utility or other electricity provider for a given premise, the applicable regulatory authority, an independent system operator (ISO) or another regional entity— that performs services or provides products using CEUD. This definition does not include Contracted Agents of an electric utility or electricity provider.

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.

This publication is available free of charge from http://dx.doi.org/10.6028/NIST.IR.7628r1

NISTIR 7628 Revision 1

Guidelines for Smart Grid Cybersecurity

Volume 3 - Supportive Analyses and References

The Smart Grid Interoperability Panel
– Smart Grid Cybersecurity Committee

http://dx.doi.org/10.6028/NIST.IR.7628r1

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

NISTIR 7628 Revision 1

Guidelines for Smart Grid Cybersecurity

Volume 3 - Supportive Analyses and References

The Smart Grid Interoperability Panel
–Smart Grid Cybersecurity Committee

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.7628r1

September 2014

U. S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology Interagency Report 7628 Rev. 1, Vol. 3
195 pages (September 2014)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: NISTIR.7628.Rev1@nist.gov

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 analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This three-volume report, *Guidelines for Smart Grid Cybersecurity*, presents an analytical framework that organizations can use to develop effective cybersecurity 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 cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

Keywords

advanced metering infrastructure; architecture; cryptography; cybersecurity; electric grid; privacy; security requirements; smart grid

ACKNOWLEDGMENTS

This revision to the NISTIR was developed by members of the Smart Grid Interoperability Panel (SGIP) Smart Grid Cybersecurity Committee (SGCC) (formerly the Cyber Security Working Group (CSWG)), which is chaired by Victoria Yan Pillitteri (NIST). Dave Dalva (Stroz Friedberg), Akhlesh Kaushiva (Department of Energy), and Scott Saunders (Sacramento Municipal Utility District) are the vice chairs and Mark Enstrom (Neustar) and Amanda Stallings (Ohio PUC) have served as the secretary. Tanya Brewer of NIST is the lead editor of this report. A special note of thanks goes to the subgroup leads, Frances Cleveland (Xanthus Consulting International), Victoria Pillitteri and Nelson Hastings (NIST), Rebecca Herold (Rebecca Herold & Associates, LLC), Elizabeth Sisley (Calm Sunrise Consulting, LLC), and Doug McGinnis (Exelon) who along with their subgroup team members contributed significantly to this revision. The dedication and commitment of all the individuals in developing the original document and now this revision is significant, especially the leadership of Marianne Swanson (NIST), who previously chaired the group. In addition, appreciation is extended to the various organizations that have committed these resources to supporting this endeavor. Past and current members of the SGCC/CSWG are listed in Appendix K of this report.

Acknowledgement is also extended to the NIST Smart Grid Team and to Liz Lennon (NIST) for her superb technical editing of this report. Thanks is also extended to Bruce McMillin (Missouri University of Science and Technology), and to Harold Booth and Quynh Dang (NIST) for assistance in updating specific sections in the document. 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

[This page intentionally left blank.]

OVERVIEW AND REPORT ORGANIZATION

REPORT OVERVIEW

This document (the original NISTIR and Revision 1) is the product of a participatory public process that, starting in March 2009, included workshops as well as weekly and bi-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 before final publication. The public review cycle were announced in The Federal Register in advance.

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 cybersecurity needs.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Document Development Strategy, Architecture, and High-Level Requirements
  - Chapter 1 – *Document Development Strategy* includes background information on the smart grid and the importance of cybersecurity in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the strategy used to develop this document.
  - Chapter 2 – *Logical Architecture and Interfaces of the Smart Grid* 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 Cybersecurity Documents*
- Appendix B – *Example Security Technologies and Services 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 – *Changing Regulatory Frameworks*
  - Appendix D – *Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties*
  - Appendix E – *Privacy Use Cases*
  - Appendix F – *Summary of Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment*
  - Appendix G - *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.
  - Chapter 8 – *Research and Development Themes for Cybersecurity 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 H – *Analysis Matrix of Interface Categories*
  - Appendix I – *Mappings to the High-Level Security Requirements Families*
  - Appendix J – *Glossary and Acronyms*
  - Appendix K – *SGIP-CSWG and SGIP 2.0 SGCC Membership*

CHAPTER 6
VULNERABILITY CLASSES

6.1 INTRODUCTION

This section is intended for use by those responsible for designing, implementing, operating or procuring any part of the electric grid. This section contains a list of four 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 exploited. 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. The following list of vulnerabilities is best used as a stimulus for detailed risk analysis of real or proposed systems since it was created from many sources of vulnerability information, including NIST Special Publication (SP) 800-82 Revision 1, *Guide to Industrial Control Systems Security* [§6.6-3], and 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations* [§6.6-2], Open Web Application Security Project (OWASP) vulnerabilities [§6.6-1], Common Weakness Enumeration (CWE) vulnerabilities [§6.6-4], 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) [§6.6-6].

6.2 PEOPLE, POLICY AND 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; adequate training ensures that people understand their role/responsibility in implementing the policy and procedures. Policy, procedures and adequately trained people are not effective without each other and should not be implemented as discreet elements. 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 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

Sufficiently trained personnel is critical to ensure that everyone in organization has a clear understanding of the importance of cybersecurity, understands their role in cybersecurity, and the importance of each role in supporting cybersecurity within the organization. Throughout the

entire organization, all personnel should have a level of security awareness training based on the individual organizational and/or the critical asset responsibilities.

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

Lack of an adequate security training and security awareness program can result in insufficiently trained personnel that do not know or understand an organization's policy framework to guard against vulnerabilities, leading to the risk of mishandled or inappropriately used information, unauthorized access to information and systems, and potentially damage to profit and organizational reputation. Security training and security awareness programs should be an ongoing effort and also include a continuous retraining effort over an organization-defined period of time to reflect new procedures, new technologies, and reinforcement of the importance of the cybersecurity program.

Potential Impact

An inadequately 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 adversaries control over the control systems.
- Holding the door for potential adversaries carrying a big box entering a "secured premise," allowing them unauthorized access and physical proximity to critical/control systems.
- Surfing porn sites, which often contain zero-day exploits that can 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 identification badges and credentials, which can be leveraged to gain partial or complete access to critical/control systems.

6.2.2 Policy and Procedures

6.2.2.1 Insufficient Identity Validation and Background Checks

Description

Insufficient identity validation and background checks may result in additional organization risk, such as theft or corporate espionage, workplace safety, unqualified or under-qualified personnel, and damage to organizational reputation. Identity validation and background checks should be based on the individual's area of responsibility, the physical facilities/hardware/systems, and the type of information authorized to access. The more sensitive information available to an individual, the deeper and more detailed the identity validation and background check process should be.

Potential Impact

The risk of insider threat, a current or former employee or Third Party who has or had authorized access to an organization's network, systems, and data and intentionally misused that access, is potential impact of insuffient identiy validation and background checks.

6.2.2.2 Inadequate Security Policy

Description

An inadequate security policy does not clearly or sufficiently define the organization's cybersecurity purpose, scope, roles, responsibilities, and compliance. Security policies must be structured with several key elements, be well-understood, embody a practical approach, be well practiced and monitored, and be enforceable. An inadequate security policy is also not reviewed and/or updated on an organizational-defined basis to allow for continuous improvement.

Potential Impact

Vulnerabilities are often introduced due to inadequate development of, implementation of, or the lack of policies. Policies should drive operating requirements and procedures, including security training.

6.2.2.3 Inadequate Privacy Policy

Description

An inadequate privacy policy does not clearly or sufficiently define the manners in which an organization gathers, uses, discloses, manages, and protects private/personal information to ensure that data is not exposed or shared unnecessarily, and what to do in the event of a breach.

Potential Impact

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

6.2.2.4 Inadequate Patch Management Process

Description

An inadequate patch management process does not sufficiently ensure that software and firmware are kept current to remediate against known vulnerabilities, or that proper risk analysis and mitigation process are 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 without additional mitigations.

6.2.2.5 Inadequate Change and Configuration Management

Description

Lack of adequate change and configuration management processes can results in system configuration that are not governed appropriately, lacking control processes for initializing, changing, and monitoring the configurations of products and systems throughout the system development lifecycle).

Examples

- Changing software configuration enables an insecure profile,
- Adding vulnerable hardware/software/firmware,
- Changing network configuration that reduces the security profile of the system,
- Introducing tampered devices into the system,
- Not having a sign-off approval in the configuration management process included in the security organization, and
- Making a change to network configuration or software 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

Unnecessary system access allows users or processes acting on behalf of users to access systems and information that is not essential to accomplishing assigned duties and tasks as required by organizational mission/business functions. System access should be managed, monitored, and enforced based on individual or process access requirements.

Potential Impact

System access that is not managed, including removal of access and accounts upon termination or transfer of personnel, 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 of;
- Individual users with sufficient access permissions to cause complete failure or failure of large portions of the electric grid;
- The 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 properly implemented risk management program facilitates more informed decision making throughout an organization, leading to more effective resource allocation, operational efficiencies, and the ability to mitigate and rapidly respond to cybersecurity risk. Ultimately, the goal of a risk management program is to reduce the likelihood and impact of a cyber event to an organization's operations, assets, and individuals.

6.2.3.1 Inadequate Periodic Security Audits

Description

An independent security audit, conducted as part of the organization's continuous monitoring program, should include review and examination of a system's records and activities to determine the adequacy of system security requirements, ensure selected security requirements are in place and operating as intended, and ensure compliance with established security policies and procedures. Audits should also be used as one of multiple security mechanisms 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; rather, be holistic reviews of processes, procedures, personnel actions, physical and network based resources that can be accomplished using automated mechanisms.

Potential Impact

The audit process can be used 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

Inadequate oversight and commitment by management can result in a suboptimal security cyberculture throughout the organization. Optimal risk management practices begin from the top

tier of the organization. Without senior management oversight and ownership, it is very difficult to maintain and fund a successful cybersecurity security program.

Potential Impact

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

An inadequate continuity of operations/disaster recovery plan can result in lacking or no procedures in place to ensure the continuation or restoration of operations in the event of a security incident. A continuity of operations/disaster recovery plan should include roles, responsibilities, training, periodic testing and exercises, and continuity of operations/disaster recovery plan updates, as well as identification of alternative storage sites, alternative command and control centers and methods, recovery and reconstitution, as well as fail-safe responses.

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

Lack of a robust risk assessment process can result in an inaccurate risk determination. This risk determination ultimately impacts the organization's understanding of what risks it faces and the associated policies, processes, and security mitigations that are implemented. A documented risk assessment process should include consideration of business objectives, the impact to the organization if vulnerabilities are exploited, and the determination of the acceptable risk level.

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 inadequate incident response process will not ensure proper notification, response, and recovery of operations and systems, and is not adequately coordinated with continuity of operations and disaster recovery capabilities.

Potential Impact

Without a sufficient incident response process, critical actions may not be completed in a timely manner, leading to increased duration of risk exposure or loss of business function.

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 adversaries 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. Discovering and reporting of vulnerability instances occur 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] The taxonomy provides a way of describing the causes of vulnerabilities, which are largely independent of the operational environment, whereas the impact of these vulnerabilities may differ in a smart grid environment compared to a traditional IT enterprise.

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 and vulnerability.

6.3.1.1 Code Quality Vulnerability (CWE-398)

Description

"Poor code quality," states the Open Web Application Security Project (OWASP),[2] "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 (CWE-778),
- Portability flaw (CWE-474, CWE-589),

[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.

[2] OWASP is a worldwide, not-for-profit charitable organization focused on improving the security of software. For more information on OWASP, refer to https://www.owasp.org/index.php/Main_Page.

- 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]

- CVE-2013-2820 - The Sierra Wireless AirLink Raven X EV-DO gateway 4221_4.0.11.003 and 4228_4.0.11.003 allows remote attackers to reprogram the firmware via a replay attack using UDP ports 17336 and 17388.
- CVE-2012-3024 - Tridium Niagara AX Framework through 3.6 uses predictable values for (1) session IDs and (2) keys, which might allow remote attackers to bypass authentication via a brute-force attack;
- CVE-2012-1799 - The web server on the Siemens Scalance S Security Module firewall S602 V2, S612 V2, and S613 V2 with firmware before 2.3.0.3 does not limit the rate of authentication attempts, which makes it easier for remote attackers to obtain access via a brute-force attack on the administrative password;
- CVE-2012-1808 - The web server in the ECOM Ethernet module in Koyo H0-ECOM, H0-ECOM100, H2-ECOM, H2-ECOM-F, H2-ECOM100, H4-ECOM, H4-ECOM-F, and H4-ECOM100 does not require authentication, which allows remote attackers to perform unspecified functions via unknown vectors;
- 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 is 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. The security of the key information may be reliant on the implementation of the mechanism (software-based vs. hardware-based) to protect the key. 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

- CVE-2012-4899 - WellinTech KingView 6.5.3 and earlier uses a weak password-hashing algorithm, which makes it easier for local users to discover credentials by reading an unspecified file;
- CVE-2012-3025 - The default configuration of Tridium Niagara AX Framework through 3.6 uses a cleartext base64 format for transmission of credentials in cookies, which allows remote attackers to obtain sensitive information by sniffing the network;

- 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 adversaries 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. Discovering 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 adversaries to change or replace the commands sent to other components.

Examples

- CVE-2012-3026 - rifsrvd.exe in the Remote Interface Service in GE Intelligent Platforms Proficy Real-Time Information Portal 2.6 through 3.5 SP1 allows remote attackers to cause a denial of service (memory corruption and service crash) or possibly execute arbitrary code via long input data,
- CVE-2012-3021 - APIFTP Server in Optimalog Optima PLC 1.5.2 and earlier allows remote attackers to cause a denial of service (infinite loop) via a malformed packet,
- 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),
- Logging of excessive data (CWE-779),
- 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

- CVE-2012-4879 - The Linux Console on the WAGO I/O System 758 model 758-870, 758-874, 758-875, and 758-876 Industrial PC (IPC) devices has a default password of wago for the (1) root and (2) admin accounts, (3) a default password of user for the user account, and (4) a default password of guest for the guest account, which makes it easier for remote attackers to obtain login access via a TELNET session,
- CVE-2012-3013 - WAGO I/O System 758 model 758-870, 758-874, 758-875, and 758-876 Industrial PC (IPC) devices have default passwords for unspecified Web Based Management accounts, which makes it easier for remote attackers to obtain administrative access via a TCP session,
- CVE-2012-3014 - The Management Software application in GarrettCom Magnum MNS-6K before 4.4.0, and 14.x before 14.4.0, has a hardcoded password for an administrative account, which allows local users to gain privileges via unspecified vectors,
- 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),
- Using password systems (CWE-309), and
- Use of default passwords.

6.3.1.12 Path Vulnerability (CWE-21)

Description

"This category [Path Vulnerability]," states OWASP, "is for tagging path issues that allow adversaries 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

The 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[3] (CWE-311, CWE-326, CWE-321, CWE-325, CWE-656),
- Lack of integrity protection for stored user data (CWE-693),

[3] OWASP, *Top 10 2007-Insecure Cryptographic Storage*, last modified April 18, 2010, http://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage [accessed 8/11/2014].

- 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 variables that include any user personal information (user name, password, home address, etc.),
- Highly protected applications should not implement mechanisms that make automated requests to prevent session timeouts,
- Highly protected applications should not implement "remember me" functionality,
- Highly protected applications should not use URL rewriting to maintain state when cookies are turned off on the client,
- Applications should not use session identifiers for encrypted HTTPS transport that have once been used over HTTP,
- Insufficient Session-ID Length (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, CWE-120)

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-2012-0227 - Buffer overflow in the VSFlex7.VSFlexGrid ActiveX control in ComponentOne FlexGrid 7.1, as used in Open Automation Software OPC Systems.NET, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long archive file name argument to the Archive method;
- CVE-2012-3035 = Buffer overflow in Emerson DeltaV 9.3.1 and 10.3 through 11.3.1 allows remote attackers to cause a denial of service (daemon crash) via a long string to an unspecified port;
- CVE-2012-5163 - Buffer overflow in an unspecified Third Party component in the Batch module for Schneider Electric CitectSCADA before 7.20 and Mitsubishi MX4 SCADA before 7.20 allows local users to execute arbitrary code via a long string in a login sequence.

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, and
- 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).

6.3.2 API Usage & Implementation

6.3.2.1 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).

6.3.2.2 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 Best Practices and Vulnerabilities

6.4.2.1 Whitelisting

Best Practice Description

The countermeasure, an application whitelist, is a list of applications and application components (libraries, configuration files, etc.) that are known to be benign. The technologies used to apply application whitelists—to control which applications are permitted to execute on a host—are called whitelisting programs, application control programs, or application whitelisting technologies. Application whitelisting technologies are intended to stop the execution of malware, unlicensed software, and other unauthorized software. Unlike security technologies such as antivirus software, which block known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other.

Examples

- Whitelisting to prevent unintentional use of software (unauthorized software, incorrect software version), and
- Signing of executables (i.e., firmware and device drivers are often signed).

6.4.2.2 File Integrity Monitoring

Best Practice Description

The countermeasure, establishing a "known and trusted" state based on a policy or standard and using a methodology or tool that finds, alerts, assesses, and acts on changes to the known state as soon as a change occurs. This ensures ongoing system integrity and automates detecting, auditing, and reconciliation of changes.

Examples

- File system integrity checking to ensure files are not changed, and
- Configuration change setting to ensure operating system settings are not changed.

6.4.2.3 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.

6.4.2.4 Installed Security Capabilities Not Enabled by Default

Description

Security capabilities must be turned on in order to be useful. There are many examples of 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.

6.4.2.5 Absent or Deficient Equipment Implementation Guidelines

Description

Unclear implementation guidelines can lead to unexpected behavior.

A system needs to be configured correctly in order 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. Guidelines for installers, operators, and managers should 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 often contains bugs and vulnerabilities. When a vulnerability is disclosed, there is often a race between adversaries and system administrators to either exploit or close the vulnerability. The security of the system using the software depends 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 choice 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 case of UNIX, an installation may automatically offer telnet, ftp, and http servers. Every service that runs is a security risk, because unintended use of the service may provide access to system assets, and the implementation may contain exploitable bugs. Services should run only if needed, and an unneeded service has no benefit and should be treated as a vulnerability.

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 an organization-defined 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 [§6.6-3, Table 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 between and 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.

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).

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, and
- Man-in-the-middle (MitM).

6.5.1.2 Inadequate Network Segregation

Description

Network architectures often do not clearly define security zones and control traffic between security zones, providing 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 adversaries 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 adversaries 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. 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 (OWASP)* [Web page], http://www.owasp.org/index.php/Category:Vulnerability [accessed 8/11/2014].
2. Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013 (including updates as of January 15, 2014), 460 pp. http://dx.doi.org/10.6028/NIST.SP.800-53r4 (redirects to: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).
3. K. Stouffer, J. Falco, and K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication (SP) 800-82 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, 170 pp. http://dx.doi.org/10.6028/NIST.SP.800-82r1 (redirects to: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf).
4. The MITRE Corporation, co-sponsored by the U.S. Department of Homeland Security, *Common Weakness Enumeration (CWE)* [Web page], http://cwe.mitre.org [accessed 8/11/2014].
5. The MITRE Corporation, co-sponsored by the U.S. Department of Homeland Security, *Common Vulnerabilities and Exposures (CVE)* [Web page], http://cve.mitre.org/ [accessed 8/11/2014].
6. North American Electric Reliability Corporation (NERC), *United States Mandatory Standards Subject to Enforcement: Critical Infrastructure Protection (CIP) Standards* [Web page], http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States [accessed 8/11/2014].
7. G. Stoneburner, C. Hayden, and A. Feringa, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* , NIST Special Publication (SP) 800-27 Revision A, National Institute of Standards and Technology, Gaithersburg,

Maryland, June 2004, 35 pp. http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf [accessed 8/11/2014].

8. CMMI Product Team, *CMMI for Development, Version 1.3*, CMU/SEI-2010-TR-033, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, Pennsylvania , November 2010, 482 pp. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9661 [accessed 8/11/2014].
9. International Organization for Standardization/ International Electrotechnical Commission, *Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)*, ISO/IEC 21827:2008. http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44716 [accessed 8/11/2014].
10. OWASP, "Testing for business logic (OWASP-BL-001)," in *OWASP Testing Guide v4*, updated April 1, 2014. http://www.owasp.org/index.php/Testing_for_business_logic_%28OWASP-BL-001%29 [accessed 8/11/2014].

CHAPTER 7
BOTTOM-UP SECURITY ANALYSIS OF THE SMART GRID

7.1 SCOPE

This section identifies specific protocols, interfaces, applications, and best practices that could and should be developed to solve specific smart grid cybersecurity problems. The section identifies some specific problems and issues that need to be addressed, but does not perform a comprehensive gap analysis that covers all possible cybersecurity issues.

Section 7.2 identifies evident and specific security problems in the smart grid that should have open and interoperable solutions, which are not solved by direct application of existing standards, de facto standards, or best practices. This illustrative list includes only cybersecurity problems that have some specific relevance to or uniqueness in the smart grid. Thus, general cybersecurity problems such as poor software engineering practices, key management, etc. are not included unless these problems have a unique challenge when considered in the context of the smart grid.

In conjunction with developing the list of specific problems, Section 7.3 identifies a list of more abstract security issues, when considered in specific contexts, can reveal specific problems.

Finally, in Section 7.4, a third list of cybersecurity design considerations for smart grid systems discusses important cybersecurity 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 do not recommend specific solutions or requirements. The 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 CYBERSECURITY PROBLEMS

This section documents specific cybersecurity problems in the smart grid by describing field cases that explain the operational, system, and device issues. The problems listed are intentionally not ordered or categorized in any particular way.

7.2.1 Authenticating and Authorizing Utility Users

This section identifies three examples of authenticating and authorizing users that is unique for the smart grid. The three examples include authenticating and authorizing utility users to substation intelligent electronic devices (IEDs), to outdoor field equipment, and to meters. In each of these examples, role-based, rather than unique user-based access control is commonly used and passwords are shared among organizational users with the same role. Also common across all of the examples is the volume of devices, leading to the same password often being used across all devices and seldom changed. Control of authentication and authorization can be centrally managed for substation IEDs, outdoor field equipment, and to meters across the utility, and is updated promptly to ensure that only intended users can authenticate to intended devices and perform authorized functions.

In the case of substation IEDs, passwords are often stored locally on the device, with different passwords allowing different authorization levels. These role passwords are shared among all users of the device performing the role, possibly including Third Party users. A device may be accessed locally and from a front panel connection, a wired network connection, or possibly via a wireless connection. The device may also be accessed remotely from a different physical location.

Substations generally have connectivity to the control center that may 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. Additionally, reliance on central authentication servers does not address certain security scenarios. For instance, authentication should continue to apply for personnel accessing devices locally in the substation when control center communications are not available. For applications where central authentication servers are in place, standby policies and procedures should also be in place and implemented in the event communications are not available.

With the infrastructure upgrades because of smart grid, some newer pole-top and other outdoor field equipment support 802.11 or Bluetooth for near-local user access for maintenance. In other cases, pole-top and other outdoor field equipment may not have connectivity to the control center and access will usually be local via wired connections, or near-local via short-range radio.

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 requirements should be in place to mitigate risk to an acceptable level. 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 addition, switchgear and other protective equipment generally have tamper detection mechanisms on doors as well as connection logging and reporting such that any unexpected or unauthorized access can be reported immediately.

For utility users (primarily maintenance personnel) accessing a meter, access may be local through the optical port of a meter or remote through the advanced metering infrastructure (AMI). 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) and cannot be assumed to be present in a maintenance scenario.

7.2.2 Authenticating Devices

Smart grid implementation will result in the interconnection of many new kinds of devices and associated challenges related to device authentication. Such scenarios include authentication between the smart meters and AMI head end, between the home area network (HAN) gateway and HAN, and the smart meters and AMI networks. In each scenario, authentication is critical to ensure that control commands are not compromised.

Authenticating communication between smart meters and an AMI head end can help ensure that an adversary cannot falsely claim to be the AMI head end and issue control commands to the meter, update firmware. Authenticating the meter to the AMI head end can help ensure that usage information is retrieved from 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.

Demand response (DR) HAN devices should 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 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 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 should be simple and user-friendly, since it will be utilized and installed by consumers who buy/rent HAN devices. HAN devices obtained by the consumer from the utility may be preprovisioned with authentication information, but HAN devices obtained from retail stores may require provisioning through an Internet connection or may receive their provisioning through the HAN gateway.

Authentication and access control is important to meters and AMI access networks (e.g., neighborhood area networks (NANs) and HANs). Network access authentication tied with access control in the AMI access networks can ensure that only authenticated and authorized entities can gain access to the NANs or HANs. In mesh networks, this functionality should be enforced at each node. The network access authentication should 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. 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. However, 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.

7.2.3 Securing Serial SCADA Communications

Many legacy substations and distribution communication systems employ 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 mechanisms to protect the integrity or confidentiality of messages, i.e., messages are transmitted in cleartext form. Solutions that wrap serial link messages into protocols like Secure Socket Layer (SSL) or Internet Protocol Security (IPsec) over Point-to-Point Protocol (PPP) include overhead imposed by such protocols, both in message payload size

and computational requirements and impact latency and bandwidth of communications on such connections.

7.2.4 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 the AMI head end is desirable, and even between HAN devices and DR control services. In both cases, for secure communication between devices, mutual authentication is also desirable.

7.2.5 Access Logs for IEDs

Not all IEDs create access logs, and due to limited bandwidth to substations, even where access logs are kept, they are often available only locally in the substation. These logs will need to become centralized and standardized so that other security tools, such as security incident and event management (SIEM) tools, can analyze the data. A solution 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 is needed.

7.2.6 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.

7.2.7 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, *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 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 using a virtual private network (VPN) connection.

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.

7.2.8 Detecting Compromised Field Devices

There should be a means to detect a penetration of a meter or group of meters in a peer-to-peer mesh environment, isolate and contain any subsequent attempts to penetrate other devices. If an adversary has the capability to reverse engineer a device, built-in protections can eventually be compromised as well. It is an open and challenging problem to perform intrusion detection in a peer-to-peer mesh environment.

7.2.9 Securing and Validating Field Device Settings

Numerous field devices contain settings, for example 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.

For example, NERC has published a *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets* that recognizes the need for protecting the system by which device settings are determined and loaded to field devices.[4] This can include the configuration management process by which the settings are determined. It is also recommended for continuous monitoring of the settings to ensure that they remain the same as intended in the configuration management process.

7.2.10 Absolute and 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 NERC Control Systems Security Working Group (CSSWG) document, *Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs*,[5] "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

[4] North American Electric Reliability Corporation (NERC), *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*, version 1.0, June 17, 2010, 47 pp. http://www.nerc.com/fileUploads/File/Standards/Critcal%20Cyber%20Asset_approved%20by%20CIPCl%20and%20SC%20for%20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf [accessed 8/11/2014].

[5] NERC, *Security Guidelines for the Electricity Sector: Time Stamping of Operational Data Logs*, version 0.995 [2009]. http://www.nerc.com/docs/cip/sgwg/Timestamping_Guideline_009-11-11_Clean.pdf [accessed 8/11/2014].

collection and analysis systems" [§7.5-14]. Some detailed examples of the importance of absolute and accurate time follow.

7.2.10.1 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. Appropriate cybersecurity measures should be in place 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.

7.2.10.2 Synchrophasors

Synchrophasor 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 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.

7.2.10.3 Certificates: Time and 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.

7.2.10.4 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 cybersecurity events. For example, correlating logs of power data from different locations can lead to enhanced understanding and analysis of disturbances and anomalies. Correlating cybersecurity events from different systems is essential to forensic analysis to determine if and how a security breach occurred and to support prosecution.

7.2.11 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 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.

7.2.12 Weak Protocol Stack Implementations

Many IP stack implementations in control systems devices are not as advanced 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.

7.2.13 Insecure Protocols

Communication protocols currently used in control systems are not typically implemented with adequate security measures. .

7.2.14 Unmanaged Call Home Functions

Many 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
- 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 CYBERSECURITY ISSUES

This subsection lists cybersecurity 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 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 due to the distributed and isolated nature of the equipment. 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 lifecycle for the electricity sector can take a year or more to qualify a patch or upgrade; there are unique challenges in how security upgrades to firmware need to be managed.

7.3.2 System Trust Model

There should be a clear idea of what elements of the system are trusted—and to what level and why. 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, one could trust a private network infrastructure more than an open public network, because the former

poses less risk. However, there are dependencies based on the design and management of that network that would inform the trust being vested in it.

7.3.3 User Trust Model

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. In terms of personnel security, it may be worthwhile considering "two-person integrity," or "TPI," 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).

7.3.4 Security Levels

A security model should 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.

7.3.5 Distributed vs. Centralized Model of Management

There are unique issues associated with how to manage a system as distributed as the smart grid, yet maintain efficiency and reliability factors that imply centralization. Many grid systems are highly distributed, geographically isolated, and require local autonomy—as commonly found in modern substations. Yet these systems need to have a measure of centralized security management in terms of event logging/analysis, authentication, etc. There should 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.

7.3.6 Intrusion Detection for Power Equipment

One issue specific to power systems is handling specialized protocols like Modbus, DNP3, IEC 61850, etc., and standardized IDS and security event detection and management models should be built for these protocols and systems. More specifically, these models should 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.

7.3.7 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. There is a need for information models and protocols that can be used over a large variety of transports and devices, bridging power equipment into traditional IT monitoring systems for their cyber aspects. The system monitoring and management interfaces will have to work within a context of massive scale, distribution, and often, bandwidth-limited connections.

7.3.8 Security Information and 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 should become centralized and analyzed for detecting events on a correlated basis. There should be clear methods of incident response to events that are coordinated between control system and IT groups, as both of these groups should be involved in security event definition. There are additional security and privacy aspects that should be considered as security event information is shared across and within organizations.

7.3.9 Trust Management

Appropriate trust of a device should be based on the physical and logical ability to protect that device, and on protections available in the network. There are many smart grid 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 should 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 should be limited accordingly. An adversary 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. 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 an intermediary 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. In this type of trust management, each system in the smart grid is categorized not only for its own needs, 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.

7.3.10 Tamper Evidence

In lieu of or in addition to tamper resistance, tamper evidence is desirable for many devices. Both tamper resistance and tamper evidence should be resistant to false positives in the form of both natural actions and adversarial actions. For example, tamper evidence for meters cannot require physical inspection of the meter, since this would conflict with zero-touch after installation, but physical indicators may be appropriate for devices in substations.

7.3.11 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.

7.3.12 Legacy Equipment with Limited Resources

The life cycle of equipment in the electricity sector typically extends beyond 20 years. Technology advances at a far more rapid rate, and security technologies typically match the trend. Legacy equipment is resource-limited, making it 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 are hindered. In many cases, the legacy device simply does not have the resources available to upgrade security on the device through firmware changes.

7.3.13 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.

7.3.14 Forensics and Related Investigations

With smart grid technology, additional threats that may require a greater capability for generating and capturing forensic data. For example, such as smart meters should be capable of detecting and reporting physical tampering to identify energy theft or billing fraud. Additionally HAN equipment will need to interact with the meter to support DR, necessitating the tools and data to diagnose problems resulting from either intentional manipulation or other causes. While it is rare that forensics 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 in accordance with legal and regulatory constraints.

7.3.15 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 should relate to the structure of the entity and its policies regarding appropriate access. Both the structure and access policies properly flow down from regulatory requirements and organizational governance.

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. 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.
3. Policies should be expressed in a manner that is implementable and relates to an entity's implemented roles.
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. Identification of devices that should to support RBAC.

7.3.16 Limited Sharing of Vulnerability and/or Incident Information

There are significant challenges with respect to sharing information about vulnerabilities or incidents in any critical infrastructure industry. There should be a framework for securely sharing such information and quickly coming to field-level mitigations until infrastructure can be upgraded. This system should also include accountability and confidentiality when sharing sensitive vulnerability information.

7.3.17 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.

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.

7.3.18 Poor Software Engineering Practices

Poor software engineering practices, such as those identified in Chapter 6 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.

7.3.19 Attribution of Faults to the Security System

When communications or services fail in networks, there is 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 should allow and support troubleshooting.

7.4 DESIGN CONSIDERATIONS

This subsection discusses cybersecurity 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 should 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

Biometrics (such as fingerprint and iris), usually used in conjunction with a token, can provide strong security authentication and access. Biometrics-based authentication is often used in high-security environments where access to the assets is required. Biometrics provides an extra level of authentication when entering a physical area or for logical access to a resource.

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 800-63-2, *Electronic Authentication Guideline* [§7.5-15], contains some

guidance on measuring password strength and recommendations for minimum password strengths.

Some considerations for password complexity rules—

1. Requirements are based on a commonly recognized standard
2. Determination that the requirements are strong enough to measurably increase the effort required to crack passwords that meet the rules.
3. If there are 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. If any hard constraints include "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. If there are 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.

7.4.4 Network Access Authentication and Access Control

Several link-layer and network-layer protocols provide network access authentication using Extensible Authentication Protocol (EAP) [§7.5-1]. EAP supports a number of authentication algorithms, also referred to as 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 Profile 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.

7.4.5 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 list 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 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.

7.4.5.1 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.

7.4.5.2 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— elated to this is the likelihood of a resource being scaled—including 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. Sharing of common costs.

7.5 REFERENCES

1. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, *Extensible Authentication Protocol (EAP)*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 3748, June 2004. http://www.ietf.org/rfc/rfc3748.txt [accessed 8/11/2014].
2. D. Simon, B. Aboba and R. Hurst, *The EAP-TLS Authentication Protocol*, IETF Network Working Group RFC 5216, March 2008. http://www.ietf.org/rfc/rfc5216.txt [accessed 8/11/2014].
3. T. Clancy and H. Tschofenig, *Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method*, IETF Network Working Group RFC 5433, February 2009. http://www.ietf.org/rfc/rfc5433.txt [accessed 8/11/2014].
4. IEEE Computer Society, *IEEE Standard for Local and Metropolitan Area Networks—Port-based Network Access Control*, IEEE Std 802.1X™-2004, December 13, 2004. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1438730 [accessed 8/11/2014].
5. IEEE Computer Society, *IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems*, IEEE Std 802.16™-2012, 2012. http://standards.ieee.org/findstds/standard/802.16-2012.html [accessed 8/11/2014].
6. D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin, *Protocol for Carrying Authentication for Network Access (PANA)*, IETF Network Working Group RFC 5191, May 2008. http://www.ietf.org/rfc/rfc5191.txt [accessed 8/11/2014].
7. Trusted Computing Group, *Trusted Network Connect (TNC)* [Web page], http://www.trustedcomputinggroup.org/developers/trusted_network_connect [accessed 8/11/2014].
8. ZigBee® Alliance [Web page], http://www.zigbee.org/ [accessed 8/11/2014].

9. C. Rigney, S. Willens, A. Rubens and W. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, IETF Network Working Group RFC 2865, June 2000. http://www.ietf.org/rfc/rfc2865.txt [accessed 8/11/2014].

10. B. Aboba, D. Simon, and P. Eronen, *Extensible Authentication Protocol (EAP) Key Management Framework*, IETF Network Working Group RFC 5247, August 2008. http://www.ietf.org/rfc/rfc5247.txt [accessed 8/11/2014].

11. D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, Washington D.C., October 27-30, 2003, pp. 52-61. http://dx.doi.org/10.1145/948109.948119.

12. K. Fehrenbacher, "Smart Meter Worm Could Spread Like a Virus," *Gigaom*, July 31, 2009. http://earth2tech.com/2009/07/31/smart-meter-worm-could-spread-like-a-virus/ [accessed 8/11/2014].

13. Department of Homeland Security, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers*, version 7, April 2011. https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf [accessed 8/11/2014].

14. North American Electric Reliability Corporation (NERC), *Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs*, version 0.995 [2009], http://www.nerc.com/docs/cip/sgwg/Timestamping_Guideline_009-11-11_Clean.pdf [accessed 8/11/2014].

15. W.E. Burr, D.F. Dodson, E.M. Newton, R.A. Perlner, W.T. Polk, S. Gupta, and E.A. Nabbus, *Electronic Authentication Guideline*, NIST Special Publication (SP) 800-63-2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2013, 123 pp. http://dx.doi.org/10.6028/NIST.SP.800-63-2 (redirects to: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf).

16. K. Stouffer, J. Falco, and K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication (SP) 800-82 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, 170 pp. http://dx.doi.org/10.6028/NIST.SP.800-82r1 (redirects to: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf).

17. K. Scarfone and M. Souppaya, *Guide to Enterprise Password Management (Draft)*, NIST Special Publication (SP) 800-118 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland, April 2009. http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf [accessed 8/11/2014].

18. K. Scarfone, C. Tibbs, and M. Sexton, *Guide to Securing WiMAX Wireless Communications*, NIST Special Publication (SP) 800-127, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2010. http://csrc.nist.gov/publications/nistpubs/800-127/sp800-127.pdf [accessed 8/11/2014].

CHAPTER 8
RESEARCH AND DEVELOPMENT THEMES FOR CYBERSECURITY IN THE SMART GRID

8.1 INTRODUCTION

Cybersecurity 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 originally produced by the R&D subgroup of SGIP-CSWG based on the inputs from various group members with updates made for the first revision of this document. 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 and does 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 cybersecurity 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 and distributed 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. 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 and 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 should 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 containment and implementing secure recovery measures using remote means.

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.

Potential starting points for these R&D efforts are

- NIST crypto tamper-evident requirements;
- Mitigating and 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 embedded systems. 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 and smart devices. Home Area Networks (HANs) provide local sensing and actuation of smart appliances. HANs and devices may communicate and negotiate in a peer-to-peer manner. 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. 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. There are cases where 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.

Encrypted communications should 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 privacy-preserving meter aggregation by

performing additive computations on encrypted data. Using aggregated data limits the ability of the utility or any Third Party from learning individual consumer usage profiles. 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, homomorphic encryption and signature schemes tailored for efficient in-network aggregation are needed.

8.3.2.3 Identity-Based Encryption

Key distribution and key revocation are some of the most fundamental problems in key distribution for systems. Identity-based encryption (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. 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

The smart grid is a long-term and expensive resource that must be built future-proof. It needs to be designed and built to adapt to changing needs in terms of scale and functionality, and at the same time, to tolerate and survive malicious attacks of the future. Research is 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 Scalability

The introduction of smart appliances and home area networks (HANs) increases the number of devices that a utility must manage by orders of magnitude. A utility with 1 million customers currently monitoring 1 million meters will conservatively see the number of devices two orders of magnitude higher (perhaps 100 million devices). The ability to control and schedule these through a central SCADA system will be severely limited. As such reliance will need to be on scheduling through HANs and distributed peer-to-peer energy management, or, an "energy internet." System vulnerabilities will be increased through the addition of potential attack points. The increased number of devices will impact system reliability and system reliability models.

8.4.2 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.

Further R&D in the area of reliability may consider the design of a wide-area distributed system (i.e., the smart grid) such that its key components and designated events have a bounded recovery and reaction time.

8.4.3 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 cybersecurity threats. However, combined with the threat environment today, such systems should a range of security measures that take into account the real-time requirements, including the overhead resulting from these security mechanisms. In some cases, security mechanisms have 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.

8.4.4 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 phasor measurement unit (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 delay sources represent security mechanisms that already exist in the system. 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 cybersecurity 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. As the smart grid scales, the ability of humans to react to systems operating in the millisecond time scale becomes limited. As such, there will need to be more reliance on embedded monitors and distributed embedded monitors to provide diagnosis and recovery actions. Without an understanding of delay-assurance tradeoffs, at times of crisis, operators may 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.

8.4.5 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; and
- Backwards compatibility, which may often be a requirement and may prevent deployment of advanced features.

Potential avenues for future investigation include:

- Compositionality (enhanced overlays, bump-in-the-wire[6], 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[7] methodology.

8.4.6 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 and mitigated. 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.

8.4.7 Efficient Composition of Mechanisms

It can sometimes be the case that even though individual components work well in their domains, compositions of them can fail to deliver the desired combination of attributes, or fail to deliver them efficiently. 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.

8.4.8 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 cybersecurity in the smart grid context raises a number of research challenges. The following subsections describe four important ones.

8.4.8.1 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.

8.4.8.2 Local Privacy

Detailed management of devices in a HAN has the potential to divulge private information both through cyber channels and also through physical channels. Recent work in Non-Intrusive Appliance Load Monitoring (NIALM) has shown very high fidelity event reconstruction through

[6] An implementation model that uses a hardware solution to implement IPSec.

[7] A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

techniques such as hidden Markov models. Significant threats to individual privacy can be envisioned (in addition to the enterprise concerns in 8.6.1.1).[8] However, privacy cannot be ensured through cryptographic methods alone.

8.4.8.3 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 of power systems.

8.4.8.4 Risk-based Cyber/Physical Security Investment

It is challenging to assess the extent to which risk has been mitigated and how much investment in cybersecurity is appropriate for a given entity in the electricity sector. Research into advanced tools and technologies based on quantitative risk notions that take into account not only cyber risks and physical risks, but combined cyber-physical risks in which cyber/physical vulnerabilities become interdependent. These include physical attacks informed by cyber in which uncovering cyber decisions leads to knowledge of physical system vulnerabilities such as congestion. These can also include cyber attacks enhancing physical attacks or a cyber system used to cause physical harm.

8.5 NETWORKING TOPICS

8.5.1 Safe Use of Commercial Off-the-shelf/Publicly Available Systems and Networks

Economic and other drivers push the use of commercial off-the-shelf (COTS) 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 reliability issues for specific types of smart grid applications. In particular, this is a quality of service issue; it is important that bandwidth is guaranteed to a distributed embedded application such as a smart grid. Considerations include the effects of delays on the physical control, for example, when physical delay or computation delay cannot be easily bounded, particularly in the face of changing network topologies and state.

[8] For more on the privacy concerns related to NIALM, see Volume 2, § 5.3.1.

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

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 and protocols 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, data link, and transport layers for SCADA, substation automation, and peer-to-peer communication.

8.5.3 IPv6

Research is needed to ensure that the IPv6-based network will be stable, reliable, and secure.

In particular, these issues need more research—

- The current and future protocols scale to millions of devices,
- Sufficiency of current modeling, simulation, and emulation technologies for future networks using IPv6,
- The validation of accuracy of projected performance,
- How devices will interoperate in multi-vendor environments,
- Identification of suitable routing protocols – either leveraging existing protocols or identifying new areas,
- Other security concerns, such as how the network be will be partitioned
- How NAT (Network Addresses Translation) should be used, and
- The need for a fundamentally new network architecture.

8.6 Other Security Issues in the Smart Grid Context

The smart grid is viewed as a cyber-physical system, hence, 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; 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 inter-organizational 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, enabling 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. Architectural solutions will be important for this objective, but there are also possibilities for improvements, for example, by using privacy-enhancing technologies based on cryptography or work on anonymity protections.
- As more information is collected, 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 better 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 and include identifying responsibility for auditing, how audit trails will be linked, and mechanisms that can be used to mine the data. 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, including research on forensic techniques to support tracing and prosecuting adversaries 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 operation of these other critical infrastructure elements. 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, 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). New security models need to be developed to overcome the limitations of purely cryptographic solutions. These models must embrace power, IT, and communications in a unified fashion;
- 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 Security Information and Event Management (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 is also need for developing new simulation capabilities for the distribution grid that incorporate communications with devices/models for distribution control, distributed generation, storage, EV/PEV/PHEV, 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.[9] 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 adversaries 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[10] (CEII), 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 extensive cyber-physical infrastructure of smart grid, 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 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. Research challenges include identification of covert network channels for smart grid systems both at the design level and when they may be exploited. Once identified, the next challenge lies

[9] B.W. Lampson, "A Note on the Confinement Problem," *Communications of the ACM* 16(10), October 1973, pp. 613-615. http://research.microsoft.com/en-us/um/people/blampson/11-Confinement/Acrobat.pdf [accessed 8/11/2014].

[10] For a list of relevant FERC Orders regarding CEII, *see* http://www.ferc.gov/legal//maj-ord-reg/land-docs/ceii-rule.asp.

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. Covert channels are not limited to network observations.

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 adversaries 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 adversaries. 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 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. The following areas of work were identified as areas of interest for further pursuit by smart grid stakeholders:

1. **Network architectures for survivability:** 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 scenario, 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. Further research in stateless packet filtering techniques may 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.

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. Additionally, NIST has published multiple publications in the area of cloud computing, which are available at: http://www.nist.gov/itl/cloud/publications.cfm.

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 should 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 should 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 and Verification Tools

The smart grid 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. Security design and verification should be a cross-domain effort and include expertise from the IT, telecom, and power systems domains.

Research and development should be conducted in security design and verification tools 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: SysML, Formal ontologies and knowledge representation based on semantic Web technologies such as Web Ontology Language (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 processes with distributed system 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. 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. It is important to identify the 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 and appropriate functional capability to act and respond to distributed security events.

Advanced security research should 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.
- Externalized security mechanisms, such as in some control system protocol implementations may be desirable because they can be scaled and upgraded independently in response to evolving threats and technology changes, possibly without retrofitting or upgrading 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.
- Functionality of some components (e.g., breakers, IEDs, relays, etc.) and communications functions should not fail due to failure of a security mechanism.
- Integration of security mechanisms between security domains is needed (for example, between logical and physical security mechanisms of remote sensors).
- 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.

- A trust model is needed to govern autonomous actions, especially by systems outside the physical control of the utility.

While it is not 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 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, including 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. This can be used to increase uncertainty and cost to adversaries.

8.6.11 Vulnerability Research

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 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. A few significant projects have undertaken security research on some of these new smart grid systems, networks, and devices, and positive results have resulted but more research is necessary. Security research grants are important 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.

8.6.13 Data Provenance

Methods to address data provenance while maintaining the operational integrity and state of many systems are needed for unique operational constraints of the smart grid. 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 operational decisions are made based on data that may have questionable attributes of confidentiality, integrity, authenticity, non-repudiation, and timeliness.
- How organizations coordinate their beliefs with other organizations, including what happens if the other organizations are suffering from a significant security breach and how one organization should 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, and 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.
- 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.

Usability of security technologies needs to improve to address these issues.

8.6.15 Cybersecurity Issues for Electric Vehicles

Plug-in electric, plug-in hybrid electric and electric vehicles (generalized in this report as PEVs) have a similar entry point to the electric grid as the smart meters and are associated with similar 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 adversaries will develop means to clone legitimate PEV interfaces for criminal activity. 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. Authentication and non-repudiation are critical in this process; otherwise a thief can use the same processes to steal a car (or disable cars as in the example, above).

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 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 9
OVERVIEW OF THE STANDARDS REVIEW

9.1 OBJECTIVE

The objective of the standards review is to ensure that identified standards applicable to the smart grid adequately address the cybersecurity requirements included in this document. If the standards do not have adequate coverage, relative to their intended scope, this review will identify where changes may need to be made or where other standards may need to be applied to provide sufficient coverage in that area. This standards review is part of the process to include a standard into the SGIP Catalog of Standards.[11]

The SGCC works with the SGIP and the standards bodies to identify the standards for review and to gain appropriate access to the standards. This is an ongoing effort as there are many standards that apply and must be assessed. To undertake the process, the CSWG/SGCC established a standards subgroup to perform the assessments and developed a review process and an assessment template for performing the assessments.

9.2 REVIEW PROCESS

9.2.1 Overview

NISTIR 7628 contains a catalog of cybersecurity requirements that can be used to identify what cybersecurity requirements are applicable to specific smart grid interactions and cybersecurity requirement families that should be considered in the review document (*see* Volume 1, Chapter 3).

9.2.2 CSWG/SGCC Review Process

Before the SGCC compares the standards document against the high-level requirements in NISTIR 7628, the SGCC reviews the scope of the standard and documents additional assumptions as to whether cybersecurity should be part of the standards document. The cybersecurity content can take the form of detailed cybersecurity technologies, specific cybersecurity requirements to meet specific cybersecurity goals, general cybersecurity best practices, or high-level policy statements. This cybersecurity content can also cover reliability/availability requirements, confidentiality requirements, data integrity requirements, and privacy issues.

Some of these requirements are general, such as having policies and procedures for specific types of interactions, for example "SG.CM-1: Configuration Management Policy and Procedures."[12] Some are more specific, such as "SG.SC-12: Use of Validated Cryptography."[13]

9.2.3 Step 1: Reviewing the Document Scope

When the SGCC receives a request from the SGIP to review a document, the SGCC reviews the scope and purpose of the requested review document, and notes any assumptions as to the

[11] For additional information on the SGIP Catalog of Standards, refer to: http://sgip.org/Catalog-of-Standards.
[12] *See* Volume 1, §3.11.
[13] *See* Volume 1, §3.24.

domain and type of document. If the document should or does contain cybersecurity requirements, then the document is assessed for cybersecurity completeness and correctness. The SGCC Standards Subgroup usually requests an expert on the document to participate and answer questions.

9.2.4 Step 2: NISTIR 7628 High-Level Cybersecurity Requirements

After assessing the overall scope of the document, the SGCC starts a detailed review of the cybersecurity contents of the document, assessing them against the High-Level Security Requirements from the NISTIR 7628. During this assessment, some requirements and interactions may not have direct correlations with the NISTIR 7628 high-level cybersecurity requirements. This will lead to a potential recommendation of:

- NISTIR 7628 high-level cybersecurity requirements may need to be updated to include them, or the requirement may be so specific that the requirement is not needed in NISTIR 7628.
- If there is a relevant NISTIR 7628 cybersecurity family or requirement that is not referenced within the scope of the review document, then a gap is documented by the SGCC and a potential recommendation is documented for the review document.

9.2.5 Step 3: Recommendations on Standard

During the assessment, cybersecurity concerns or issues are noted and often discussed with the owners of the document. Recommendations for improvement on cybersecurity issues are provided so that the document owners may choose to update the document or undertake additional documents to address these recommendations.

If the standard meets all relevant requirements, the SGCC recommends inclusion in the SGIP Catalog of Standards. If some requirements are not met, the SGCC may recommend conditional approval pending the correction or mitigation of the cybersecurity concern.

9.3 SGCC Standards Assessment Concepts

The following provides the background and concepts used in assessing standards:

9.3.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the smart grid are designed to meet many different requirements at many different "layers" in the reference model. Two commonly used reference models are the International Organization for Standardization (ISO)/Open Systems Interconnection model (OSI) 7-layer reference model[14] and the GridWise Architecture Council (GWAC) Stack[15] (see Figure 9-1), where the OSI 7-layer model maps to the Technical levels of the GWAC Stack. Some standards address the lower layers of the reference models, such as

[14] International Organization for Standardization/International Electrotechnical Commission, *Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*, ISO/IEC 7498-1:1994.

[15] The GWAC Stack is available at http://www.gridwiseac.org/ in the *GridWise Interoperability Context-Setting Framework.*

wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Cybersecurity is a cross-cutting issue and should be reflected in requirements at all levels: cybersecurity policies and procedures mainly cover the GWAC Stack Organizational and Informational levels, while cybersecurity technologies generally address those requirements at the Technical level.

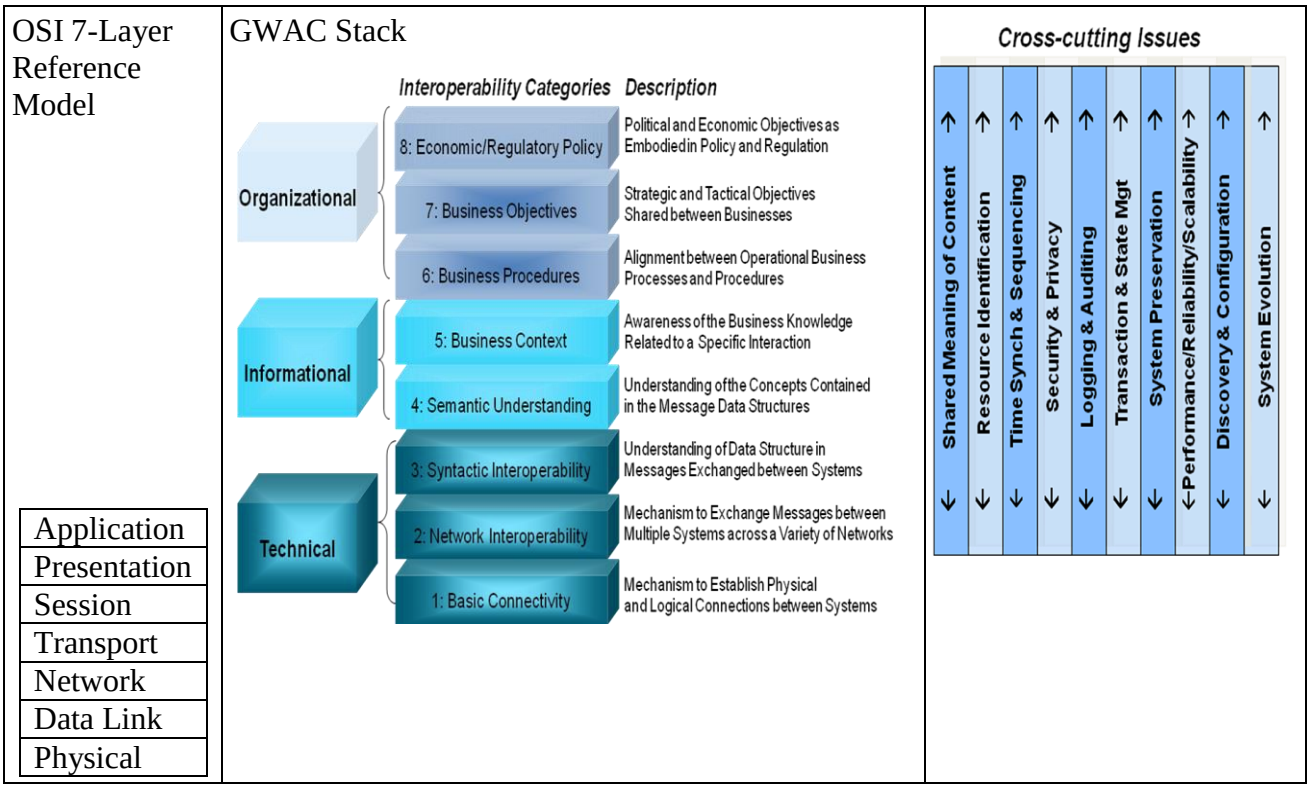


Figure 9-1 ISO/OSI 7-Layer Reference Model and GWAC Stack Reference Model

Second, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Third, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself - how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of policy, procedural, and communication standards designed to provide specific services. Ultimately cybersecurity, as applied to the information exchange standards, should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g., encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if Transmission Control Protocol (TCP)/Internet Protocol (IP) is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then transport layer security (TLS) should be used.

In the following discussions of information exchange standard being reviewed, these caveats should be taken into account.

9.3.2 Correlation of Cybersecurity Requirements with Physical Security Requirements

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent adversaries from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may be used to help protect the other, while compromises of one can definitely compromise the other.

Physical and environmental security that encompasses protection of physical assets from damage is addressed by this document only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

9.3.3 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as "appropriate security technologies and procedures should be implemented."

With the advent of the smart grid, cybersecurity has become increasingly important within the electricity sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards

may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

9.3.4 References and Terminology

References to NISTIR 7628 security requirements refer to Volume 1, Chapter 3, High-Level Security Requirements, of this document.

References to "government-approved cryptography" refer to the list of approved cryptography suites identified in Volume 1, Chapter 4, Cryptography and Key Management, of this document. Summary tables of the approved cryptography suites are provided in Volume 1, §4.3.2.1.

Some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

The terms "approved", "acceptable", and "deprecated" are defined as the following:[16]

- Approved is used to mean that an algorithm is specified in a FIPS or NIST Recommendation (published as a NIST Special Publication).
- Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known.
- Deprecated means that the use of the algorithm and key length is allowed, but the user must accept some risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature).

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[17]:

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (shall equals is required to).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (should equals is recommended that).

---

[16] The definitions are obtained from NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, available at http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf [accessed 8/11/2014].

[17] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (may equals is permitted to).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (can equals is able to).
- The use of the word must is deprecated, and should not be used in these standards to define mandatory requirements. The word must is only used to describe unavoidable situations (e.g., "All traffic in this lane must turn right at the next intersection.")

9.4 SGCC STANDARDS ASSESSMENT TEMPLATE

The following presents the standards assessment template, including the template structure and questions, used by the Standards Subgroup to report findings from their standards review effort.

1. **Description of Document**
2. **Assumptions**
3. **Assessment of Cybersecurity Content**
4. **Does the standard address cybersecurity? If not, should it?**
5. **What aspects of cybersecurity does the standard address and how well (correctly) does it do so?**

Table 9-1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard	Applicable NISTIR 7628 High Level Security Requirements	Comments including how NISTIR HLR Requirements Are or Are Not Completely Met

6. **What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?**
7. **What work, if any, is being done currently or is planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?**
8. **Recommendations**

   The SGCC recommends {specific recommendations from the SGCC on the standard}

9. **List any references to other standards and whether they are normative or informative**

CHAPTER 10
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. The Use Cases presented in this chapter will be employed in evaluating smart grid characteristics and associated cybersecurity objectives; the high-level requirements of confidentiality, integrity, and availability (CIA); 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 chapter 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, Directory of Use Cases[18].
- **AMI Business Functions**: Use Cases were originally 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 – Smart Grid Cybersecurity Committee (SGIP-SGCC) has now also posted this material on the SGIP TWiki). Before the revision of this document, the CSWG/SGCC AMI Subgroup revised the AMI use cases to better reflect actual AMI deployments.
- **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.

[18] http://www.intelligrid.info/scripts/dir_list_sort.asp.

- **EPRI Use Case Repository**: A compilation of IntelliGrid and Southern California Edison (SCE) Use Cases, plus others. See EPRI Web site, Use Case Repository[19].
- **SCE Use Cases**: Developed by Southern California Edison with the assistance of EnerNex. *See* SCE.com Web site, Use Case Series Descriptions[20].

A certain amount of overlap is found in these sources, particularly in the new area of AMI. However, even the combined set (numbering over 1,000 Use Cases) does not address all requirements. For example, for one operation—the connect/disconnect of meters—originally 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 10.3 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 10.2.1 through 10.2.3.

10.2.1 CI&ASecurity 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,
- Timestamp associated with the data is known and authenticated,
- Quality of data is known and authenticated.

[19] http://www.smartgrid.epri.com/Repository/Repository.aspx

[20] https://www.sce.com/wps/portal/home/customer-service/my-account/smart-meters/use-case-license-agreement/!ut/p/b1/hdDBroIwEAXQb_EHmJEq4LIahCpaeBDAbgyaWlGkBo38vpg8F8aos5vk3EnugIAcRF3cSlVcS10X1WMX1rrveNRnMTJusimyv0XAo5Bj6JIOrDqAH4bir3wG4pU4czJANh64CZ-YaFvkDQSp3QEvjtIwRT-wf4DF88LIQ9efcWReEhFkJMJlTClBtP7BlxYzEKrSm-4j2RjEypTJUD2603pDHAWikTvZyMbY68sV8rZtDaW1qqSx1Sc4n3Is2WF4zGjvDvu-np8!/dl4/d5/L2dBISEvZ0FBIS9nQSEh/.

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

In this chapter basic use cases are described which can be used as building blocks for more complex use cases that users of this guideline and AMI security profile may be interested in. Dozens of use cases can be constructed from these basic functions. A few short examples are provided below that demonstrate a more detailed process of combining the basic building blocks in the AMI security profile.

There are other functions not specified below which can be composed from these defined functions. The absence of a function on the list of use cases should not be taken as indication those functions are less important, but as an indication those functions are combinations of basic functions with the possible addition of out-of-scope and/or business process behaviors. Some examples:

- Revenue Protection: Revenue protection with respect to AMI consists of a number of business processes combined with AMI functions. For example, theft of service can be identified by comparing meter reads (Meter Sends Information function) of power line branch meter with the sum of meter reads of each of the subscribers on that branch (a specific non-AMI business process). A discrepancy on the total can indicate theft of service.

- Meter Removal: Detection of meter removal can occur in a number of different ways including "Meter Sends Information" where the exception case indicates no contact with the meter or "Meter Sends Alarm" where the self-protection capability of the meter notes a tamper event. There is also the case that includes meter not communicating (disassociated from network), where a meter that has been associated or registered on the network is no longer performing necessary activities to maintain registration.

- Meter Bypass: Generically, detection of meter bypass is a back office business process dependent on information received from the field. One way of detecting meter bypass is historical analysis of consumption data and comparison of that data to other similar subscribers in the region.

- Outage Detection and Restoration: This is not directly an AMI function, but information for the process can be acquired from the AMI meter field through the "Meter Sends Information" function and the "Meter Sends Alarm" function. Depending on the needs of restoration, "Utility Sends Operational Command" may also occur. The specific set of functions for detection and restoration will most likely be different with each outage event and may differ based on the Utility and its practices.

- Pre-paid Metering: Depending on the specific mechanism for pre-paid metering (e.g., payment at the meter, payment to the utility, emergency power enable button) this can end up being the combination of any or all AMI functions. At the simplest, the setting of a consumption limit on a meter based on some business process decision by the utility would be a "Utility Sends Operational Command". Information about consumption rates as well as warnings about credit exhaustion will flow back to the utility via "Meter Sends Information" and "Meter Sends Alarm".

The 6 basic functions listed below were chosen because they mostly represent the same level of control plane and they involve only AMI elements. As utilities continue to develop their set of use cases, which involve (but are not necessarily limited to) AMI elements, they can use this set of functions to describe the AMI portion of the use case.

<table>
<tr><td colspan="2">Category: AMI</td><td>Overall Use Case #1</td></tr>
<tr><td colspan="3">Scenario: Meter sends information</td></tr>
<tr><td colspan="3"><u>Category Description</u>
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.</td></tr>
<tr><td colspan="3"><u>Scenario Description</u>
A meter sends automated energy usage information to the Utility (e.g., meter read (usage data)). The automated send of energy usage information is initiated by the meter and is sent to the Advanced metering Infrastructure (AMI) Head End System (HES). The Head End system message flows to the meter Reading and Control (MRC). The MRC evaluates the message. The MRC archives the automated energy usage information and forwards the information onto the meter Data Management Systems (MDMS).
Meter configuration information
Periodic meter Reading
On-Demand meter Reading
Net metering for distributed energy resources (DER) and plug in electric vehicle (PEV)</td></tr>
<tr><td><u>Smart Grid Characteristics</u>
Enables active participation by consumers
Enables new products, services and markets
Optimizes asset utilization and operate efficiently</td><td><u>Cybersecurity Objectives/Requirements</u>
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</td><td><u>Potential Stakeholder Issues</u>
Customer data access
Customer data privacy and security
Reliable data for billing
Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services
Third party or party acting on behalf of the utility reliable data</td></tr>
</table>

Category: AMI	Overall Use Case #2
Scenario: Utility sends operational command to 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

A Utility requires an operational command be sent to the meter, such as a disconnect or reconnect of an electric smart meter. The command flows to the meter Reading and Control (MRC) that looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to communicate the command to the meter. The HES evaluates current conditions and, if suitable (e.g., reconnects are not executed if the system is in a rolling black out state), sends the command to the meter. When the meter receives the command and parameters, the meter evaluates the command as to whether it is permitted. If the command is permitted, the meter executes the command and sends the result to the HES. If the command is not permitted, the meter sends the result to the HES. The HES evaluates the result (whether the action was successful or not and why) and relays that to the MRC. The MRC records the command result and notifies the appropriate actors.

- Configuration request
- Calibration request
- Connect / Disconnect request
- Prepaid metering configuration/setup

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters	• Confidentiality requirements of the meter command is generally not very important • Integrity of control commands to the meter is critical to avoid dangerous/unsafe conditions. • Availability is not important with the exception of emergency situations such as fire or medical emergency for remote connect/disconnect.	• Customer Safety • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services

Category: AMI	Overall Use Case #3
Scenario: Field tool sends instruction to the 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

A field tool requires onsite maintenance of an electric smart meter. The Field Tool connects directly to an electric smart meter, then the command flows to the smart meter. When the meter receives the command and parameters, the meter evaluates the command as to whether it is permitted. If the command is permitted, the meter executes the command and sends the result back to the field tool. This use case is a closed loop, as stated in the preconditions.

- Meter calibration update
- Meter configuration update

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Enables new products, services and markets	• Confidentiality is not important unless some maintenance activity involves personal information • Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions and integrity of billing data to prevent high utility bills • Availability is important, because field tool requires real time interaction with the meter.	• Customer data privacy and security • Third party or party acting as an agent of the utility having access to customer & Utility information

Category: AMI	Overall Use Case #4
Scenario: Utility sends non-operational instruction to meter (peer-to-peer)	

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

This use case describes the Utility sending a non-operational instruction sent to meter as a peer-to-peer transaction. A Utility requires actions from a set of meters, which may or may not result in a change to the power state of the grid. These include at least meter reading, and certain configuration changes. The meter Reading and Control (MRC) determines the need to send instruction(s) to a meter. MRC looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to queue up and execute the instruction(s). The AMI Head End can determine the instruction needs to be split into packets, schedules the sending of the packets and continues to send the packets to the meter until all instruction packets have been sent. The meter receives the instruction(s) and determines if the instruction is permitted. After execution, the meter sends the instruction result to the HES. The HES will then send the instruction result to the MRC. If the instruction result is energy usage information, the MRC will then forward the energy usage information onto the meter Data Management System (MDMS). If the MDMS receives energy usage information, then the MDMS forwards the energy usage information onto other actors for other actions.

- Meter calibration validation
- Connectivity validation
- Geolocation of meter
- Smart meter battery management

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Operates resiliently in response to natural and manmade events • Increases the timeliness, availability, and granularity of information for billing	• Confidentiality may or may not be an issue depending on whether information is public (date, time) or private (password change, Personal Identifiable Information). Some items must be confidential due to laws and regulations; confidentiality of other items may be left up to local policy, such as firmware or GPS coordinates. • Integrity of meter maintenance repairs and updates is essential to prevent malicious intrusions • Availability is important, but only in terms of hours or maybe days to provide synchronization and coherence of devices on the network, i.e., all devices acting together for entire population	• Customer data privacy and security • Third party or party acting as an agent of the utility having access to customer & Utility information • Third party access to electrical distribution system, e.g., separation of duties & authority (regulatory impact) • Vendor product quality

Category: AMI	Overall Use Case #5
Scenario: Utility sends batch instruction to meters (group multicast transaction)	

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

This use case describes a batch instruction send to meters as a multicast transaction in an open loop situation. The open loop situation means that Advanced metering Infrastructure (AMI) Head End System (HES) does not expect a response for each packet sent to a meter. A Utility requires actions from a set of meters, which may or may not result in a change to the power state of the grid. These include at least meter reading, and certain configuration changes. The meter Reading and Control (MRC) determines the need to send batch instructions to more than one meter. MRC looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to queue up and execute the instructions. The AMI Head End can determine the instruction needs to be split into packets, schedules the sending of the packets and continues to send the packets to the meters until all instruction packets have been sent. The meter(s) receive the instruction(s) and determines if the instruction is permitted. After execution, the meter(s) send the instruction result to the HES. The HES will then send the instruction result to the MRC. If the instruction result is energy usage information, the MRC will then forward the energy usage information onto the meter Data Management System (MDMS). If the MDMS receives energy usage information, then the MDMS forwards the energy usage information onto other actors for other actions.

- Firmware update
- Key management update

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Enables new products, services and markets • Reduces cost of operations	• Confidentiality is not important unless some maintenance activity involves personal information • Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions • Availability is important, but only in terms of hours or maybe days	• Confirmation (if required) of update status. • Customer data privacy and security • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services

Category: AMI	Overall Use Case #6
Scenario: Meter sends alarm or unsolicited and unscheduled request to the utility	
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 A meter sends an alarm or unsolicited and unscheduled request to the Utility (e.g., Physical tamper detection, Network join request, or HAN device / direct load control device enrollment request (proxy for customer). The message is initiated by the meter and sends the messages to the Advanced metering Infrastructure (AMI) Head End System (HES). The HES message flows to the meter Reading and Control (MRC). The MRC evaluates the message. The MRC records the command result and notifies the appropriate actors.	

Smart Grid Characteristics	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters	• Confidentiality is not important unless alarm contains private information or exposes an attempt to obtain security information stored in the meter • Integrity - Protect against energy theft • Protect integrity of meter configuration • Protect integrity of reporting • To protect the integrity of the network (authorized devices) • Availability is important to capture last gasp detecting, join detection, and reporting	• Network Service Providers • Customer may receive outage notification through Third Party • Billing service provider • Transmission & Distribution service provider

10.3.2 Demand Response Security Use Cases

<table>
<tr><td colspan="2">Category: Demand Response (DR)</td><td>Overall Use Case #7</td></tr>
<tr><td colspan="3">Scenario: Real-Time Pricing (RTP) for Customer Load and DER/PEV</td></tr>
<tr><td colspan="3"><u>Category Description</u>
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.</td></tr>
<tr><td colspan="3"><u>Scenario Description</u>
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.</td></tr>
<tr><td><u>Smart Grid Characteristics</u>
• Enables active participation by consumers
• Accommodates all generation and storage options
• Enables new products, services and markets</td><td><u>Cybersecurity Objectives/Requirements</u>
• 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</td><td><u>Potential Stakeholder Issues</u>
• Customer data privacy and security
• Retail Electric Supplier access
• Customer data access</td></tr>
</table>

Category: Demand Response	Overall Use Case #8
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	**Cybersecurity 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	Overall Use Case #9
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	**Cybersecurity 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	Overall Use Case #10
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	**Cybersecurity 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	Overall Use Case #11
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	Cybersecurity 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	Overall Use Case #12
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	**Cybersecurity 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

<table>
<tr><td colspan="2">Category: Customer Interfaces</td><td>Overall Use Case #13</td></tr>
<tr><td colspan="3">Scenario: Customer’s In Home Device is Provisioned to Communicate With the Utility</td></tr>
<tr><td colspan="3"><u>Category Description</u>
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.</td></tr>
<tr><td colspan="3"><u>Scenario Description</u>
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.</td></tr>
<tr><td><u>Smart Grid Characteristics</u>
• Enables active participation by consumers
• Accommodates all generation and storage options
• Enables new products, services and markets</td><td><u>Cybersecurity Objectives/Requirements</u>
• To protect passwords
• To protect key material
• To authenticate with other devices on the AMI system</td><td><u>Potential Stakeholder Issues</u>
• Customer device standards
• Customer data privacy and security</td></tr>
</table>

Category: Customer Interfaces	Overall Use Case #14
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	**Cybersecurity 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	Overall Use Case #15
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	**Cybersecurity 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	Overall Use Case #16
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	**Cybersecurity 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	Overall Use Case #17
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	**Cybersecurity 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	Overall Use Case #18
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	**Cybersecurity 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

<table>
<tr><td colspan="2">Category: Electricity Market</td><td>Overall Use Case #19</td></tr>
<tr><td colspan="3">Scenario: Bulk Power Electricity Market</td></tr>
<tr><td colspan="3"><u>Category Description</u>
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.</td></tr>
<tr><td colspan="3"><u>Scenario Description</u>
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.</td></tr>
<tr><td><u>Smart Grid Characteristics</u>
• Enables active participation by consumers
• Accommodates all generation and storage options
• Enables new products, services and markets</td><td><u>Cybersecurity Objectives/Requirements</u>
• 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</td><td><u>Potential Stakeholder Issues</u>
• Customer data privacy and security
• Retail Electric Supplier access
• Customer data access</td></tr>
</table>

Category: Electricity Market	Overall Use Case #20
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	**Cybersecurity 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	Overall Use Case #21
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	Cybersecurity 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)	Overall Use Case #22	
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 • 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	**Cybersecurity Objectives/Requirements** • 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	**Potential Stakeholder Issues** • Customer safety • Device standards • Cybersecurity

Category: Distribution Automation	Overall Use Case #23
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	**Cybersecurity 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	Overall Use Case #24

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	**Cybersecurity 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	Overall Use Case #25

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

Category: Distribution Automation	Overall Use Case #26
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	**Cybersecurity 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	Overall Use Case #27

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

Category: Distribution Automation	Overall Use Case #28

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

Category: Distribution Automation	Overall Use Case #29
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	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity not critical due to multiple sources of data • Availability is not important • Confidentiality is not important	• Cybersecurity

10.3.6 PHEV Security Use Cases

Category: Plug-In Hybrid Electric Vehicles (PHEV)	Overall Use Case #30
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	**Cybersecurity 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	Overall Use Case #31
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	**Cybersecurity 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	Overall Use Case #32
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	**Cybersecurity 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	• Improved system stability and availability • To keep customer information private • To insure DR messages are accurate and trustworthy	• Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Plug-In Hybrid Electric Vehicles	Overall Use Case #33
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	**Cybersecurity 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	• Improved system stability and availability • Pricing signals are accurate and trustworthy • Customer information is kept private	• Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

10.3.7 Distributed Resources Security Use Cases

Category: Distributed Resources	Overall Use Case #34
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	**Cybersecurity 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	Overall Use Case #35
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	**Cybersecurity Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently	• Commands are trustworthy and accurate • Customer's data is kept private • DR messages are received timely	• Safety • Customer data privacy and security

10.3.8 Transmission Resources Security Use Cases

<table>
<tr><td>Category: Transmission Operations</td><td>Overall Use Case #36</td></tr>
<tr><td colspan="2">Scenario: Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data</td></tr>
<tr><td colspan="2"><u>Category Description</u>
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.</td></tr>
<tr><td colspan="2"><u>Scenario Description</u>
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</td></tr>
<tr><td><u>Smart Grid Characteristics</u>
• Provides power quality
• Optimizes asset utilization
• Anticipates and responds to system disturbances</td><td><u>Cybersecurity Objectives/Requirements</u>
• 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</td><td><u>Potential Stakeholder Issues</u>
• Customer safety
• Customer device standards
• Demand response acceptance by customers</td></tr>
</table>

Category: Transmission Operations	Overall Use Case #37
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	**Cybersecurity 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	• Cybersecurity

Category: Transmission Operations	Overall Use Case #38

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	**Cybersecurity 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	Overall Use Case #39
Scenario: Wide Area Synchrophasor 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	**Cybersecurity 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	• Cybersecurity • Customer data privacy and security

10.3.9 RTO/ISO Operations Security Use Cases

Category: RTO/ISO Operations	Overall Use Case #40
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	**Cybersecurity 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 operator commands (e.g., one second) • Confidentiality is not important	• Cybersecurity • Customer data privacy and security

10.3.10 Asset Management Security Use Cases

Category: Asset Management	Overall Use Case #41
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	**Cybersecurity 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 • Cybersecurity

Category: Asset Management	Overall Use Case #42
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	**Cybersecurity 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	• Cybersecurity • Customer data privacy and security

Category: Asset Management	Overall Use Case #43
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	**Cybersecurity 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	Overall Use Case #44
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	**Cybersecurity 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	• Cybersecurity • Customer data privacy and security

APPENDIX H
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 H-1 provides additional descriptions of each attribute.

Table H-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 that 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 that 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 that 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 H-2 provides the analysis matrix of the security-related logical interface categories (rows) against the attributes (ATR) that reflect the interface categories (columns).

Table H-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
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

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
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				
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				

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

I.1 VULNERABILITY CLASSES

The following is a mapping of vulnerability classes [See §6] to the High-Level Security Requirements Families.

Table I-1 Mapping of Vulnerability Classes to 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, and 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					

			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		Inadequate Patch Management Process	X			X	X	X	X							X			X	X	
		Inadequate Change and Configuration Management				X										X				X	
		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 Incident Response Process				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	Code Quality Vulnerability		X								X				X		X	X	X	X
	Authentication Vulnerability		X	X			X								X			X	X	X
	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
	Business 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

			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	Path Vulnerability		X												X				X	X
		Protocol Errors		X												X				X	X
		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		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)
		Defined, or "Illegal" Conditions																			
		Use of Insecure Protocols		X												X		X		X	X
		Weakness that Affect Files and Directories		X												X				X	X
	API Usage & Implementation	API Abuse		X												X				X	X
		Use of Dangerous API		X												X				X	X
Platform Vulnerabilities	Design	Use of Inadequate Security Architecture and Designs	X	X	X		X	X	X			X		X		X	X	X	X	X	X
		Lack of External or Peer Review for Security Design	X	X	X		X	X	X			X		X		X	X	X	X	X	X
	Impl eme	Whitelisting Best Practice)			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)
	File Integrity Monitoring (Best Practice)								X	X								X	X	X
	Inadequate Malware Protection		X	X		X		X					X			X	X	X	X	
	Installed Security Capabilities Not Enables by Default	X	X	X	X		X						X			X	X	X	X	
	Absent or Deficient Equipment Implementation Guidelines	X	X	X	X		X						X		X	X	X		X	
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	

			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)
	Poorly configured security equip.	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	X
		Weakness in Authentication Process or Authentication Keys				X														X	X
		Insufficient Redundancy	X			X		X				X	X		X	X					X
		Physical Access to the Device	X			X		X				X	X		X	X				X	X

I.2 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.

Table I-2 Mapping of Bottom-Up Topics 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)
Authenticating and Authorizing Utility Users to Substation IEDs						X													
Authenticating Devices						X													
Securing Serial SCADA Communications																X			
Secure End-to-End Meter to Head End Communication																X			
Access Logs for IEDs			X																
Remote Attestation of Meters																X	X		X
Outsourced WAN Links																X			
Detecting Compromised Field Devices																	X	X	
Securing and Validating Field Device Settings	X					X										X			
Absolute and Accurate Time Information			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)
Security Protocols																			
Synchrophasors																			
Certificates: Time and Date Issues																			
Event Logs and Forensics																			
Security for Radio-Controlled Distribution Devices						X										X			
Weak Protocol Stack Implementations																X			
Insecure Protocols																			
Unmanaged Call Home Function																			
Patch Management																	X		
System Trust Model																X			
User Trust Model																X			
Security Levels																			
Distributed versus Centralized Model of Management																			
Intrusion Detection for Power Equipment				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)
Network and System and Management for Power Equipment	X			X		X											X		
Security Information and Event Management					X		X										X		X
Trust Management																			
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					
Traffic Analysis						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)
Poor Software Engineering Practices																	**X**		
Attribution of Faults to the Security System																			
Need for Unified Requirements Model																			
Break Glass Authentication																			
Biometrics	**X**					**X**													
Password Complexity Rules	**X**					**X**													
Network Access Authentication and Access Control	**X**					**X**													

I.3 R&D TOPICS

The following table is a mapping of research and development topics [See §8] to the High-Level Security Requirements Families.

Table I-3 Mapping of R&D Topics to the High-Level 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		
	Advanced Topics in Cryptography									X							X	X		
Systems	Scalability				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)
	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			
	Risk Assessment and Management				X	X		X						X	X	X				
Networking	Safe use of COTS/Publicly Available																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)
Other Security Issues in the Smart Grid Context	Systems and Networks																		
	Advanced Networking																X		
	IPv6																X		X	X
	Privacy and Access Control in Federated Systems	X		X			X												
	Auditing and Accountability			X															
	Infrastructure Interdependency Issues					X		X					X			X				
	Cross-Domain (Power/Electrical to Cyber/Digital) Security Event Detection, Analysis, and Response					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)
Other Security Issues in the Smart Grid Context	Covert Network Channels in the Smart Grid: Creation, Characterization, Detection and Elimination					X		X									X			
	DoS Resiliency	X				X	X	X									X	X		
	Cloud Security	X					X		X	X							X			
	Security Design and Verification Tools				X															X
	Distributed versus Centralized security	X			X	X	X	X							X		X	X	X	
	System Segmentation and Virtualization	X			X					X							X	X		X
	Vulnerability Research	X	X		X		X			X	X	X		X			X	X	X	X
	Vulnerability Research Tools	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)
	Data Provenance			X	X		X			X							X	X		X
	Security and Usability		X												X	X				
	Cybersecurity Issues for Electric Vehicles	X		X			X			X							X	X		X
	Detecting Anomalous Behavior Using Modeling			X	X			X									X	X		

APPENDIX J
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	An 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/PEV/PHEV	Electric Vehicle/Plug-in 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. 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
SEP	Smart Energy Profile
SGCC	Smart Grid Cybersecurity Committee
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

SIEM	Security Information and Event Management (SIEM)
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 public key infrastructure, 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 K
SGIP-CSWG AND SGIP 2.0-SGCC MEMBERSHIP

This list is a combination of all participants in the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG, including all of the subgroups) and the SGIP 2.0 Smart Grid Cybersecurity Committee. Some of the organizations listed have changed over time, but these reflect the organizational affiliation of the members during their time of membership.

Name	Organization
Aber, Lee	OPOWER
Ackerman, Eric	Edison Electric Institute
Ahmad, Wadji	General Electric
Ahmadi, Mike	GraniteKey
Ahsan, Naeem	DNV KEMA Energy and Sustainability
Aikman, Megan	FERC
Akyol, Bora	Pacific Northwest National Laboratory
Alcaraz, Cristina	NIST
Alexander, Michael	Underwriters Laboratories Inc.
Alexander, Rob	Ember Corporation
Alexander, Roger	Eka Systems, Inc.
Allitt, Ed	IPKeys
Al-Mukdad, Wendy	California PUC
Alrich, Tom	ENCARI
Ambady, Balu	Sensus
Anderson, Casey	Tendril, Inc.
Anderson, Dwight	Schweitzer Engineering Labs
Anderson, Ken	Information and Privacy Commissioner's Office of Ontario
Andreou, Demos	Cooper Industries
Andrews, Joseph	Western Electricity Coordinating Council
Antonacopoulos, Glenn	Northrop Grumman Corp.
Arensman, Will	SouthWest Research Institute
Arneja, Vince	Arxan Technologies, Inc.
Artz, Sharla	Schweitzer Engineering Laboratories
Arunachalam, Arun	Southern California Edison
Ascough, Jessica	Harris Corporation
Ashton, Skip	Ember Corporation
Bacik, Sandy	Enernex

Baiba Grazdina	Duke Energy
Baker, Fred	Cisco Systems, Inc.
Balsam, John	Georgia Tech Research Institute
Banerjee, Aditi	Texas Instruments
Barber, Mitch	Industrial Defender, Inc.
Barclay, Steve	ATIS
Barnes, Frank	University of Colorado at Boulder
Barnett, Bruce	GE Global Research
Barr, Michael	L-3 Communications Nova Engineering
Bartol, Nadya	Utilities Telecom Council
Barton, Michael	SunPower Corporation
Bass, Len	Software Engineering Institute Carnegie Mellon University
Basu, Sourjo	General Electric Energy
Bates, Shirley	Siemens
Batz, David	Edison Electric Institute
Beale, Steven	Future of Privacy Forum
Behrens, Stephen	KEMA, Inc.
Beinert, Rolf	OpenADR
Belanger, Phil	Oak Tree Consulting
Belgi, Subodh	MIEL e-Security Private Limited
Bell, Ray	Grid Net
Bell, Will	Grid Net
Bemmel, Vincent	Trilliant
Bender, Klaus	Utilities Telecom Council
Benn, Jason	Hawaiian Electric Company
Benoit, Jacques	Cooper Power Systems
Berkowitz, Don	S&C Electric Company
Beroset, Ed	Elster Group
Berrett, Dan E.	DHS Standards Awareness Team (SAT)
Berrey, Adam	General Catalyst Partners
Bertholet, Pierre-Yves	Ashlawn Energy, LLC
Besko, Geoff	Seccuris, Inc.
Beyene, Tsegereda	Cisco Systems, Inc.
Bezecny, Steve	CenterPoint Energy
Bhaskar, Mithun M.	National Institute of Technology, Warangal
Biggs, Doug	Infogard

Biggs, Les	Infogard
Bilow, Steve	The Bilow Group
Bitter, David	SMUD
Blomgren, Paul	SafeNet Inc.
Blossom, Michael	SmartSynch
Bobba, Rakesh	University of Illinois, Urbana-Champaign
Bochman, Andy	IBM
Bockenek, Richard	Verizon
Boivie, Rick	IBM T. J. Watson Research Center
Boulez, Kris	Ascure
Brackney, Dick	Microsoft
Bradley, Steven	Virginia State Corporation Commission
Braendle, Markus	ABB
Branco, Carlos	Northeast Utilities
Brennan, Jim	New Hampshire PUC
Brent, Richard	FriiPwrLtd
Brenton, Jim	Ercot
Brewer, Tanya	NIST
Brigati, David	NitroSecurity
Brinskele, Ed	Vir2us Inc.
Brooks, Thurston	3e Technologies International, Inc.
Brown, Bobby	Consumers Energy / EnerNex Corporation
Brown, Peter	Progress Energy
Brozek, Mike	Westar Energy, Inc.
Brunnetto, Michael	
Bryan, Clifford	Examiner.com
Brydl, Jerry	Steffes Corporation
Bucciero, Joe	Buccerio Consulting
Buffo, Lydia	Dominion
Bump, William	Booz, Allen, Hamilton
Burnham, Laurie	Dartmouth College
Butler, Greg	
Butterworth, Jim	Guidance Software
Byrum, Drake	Cigital, Inc.
Camilleri, John	Green Energy Corp
Camm, Larry	Schweitzer Engineering Laboratories, Inc.
Campagna, Matt	Certicom Corp.

Cam-Winget, Nancy	Cisco Systems, Inc.
Caprio, Daniel	McKenna Long & Aldridge LLP
Cardenas, Alvaro A.	Fujitsu
Carlson, Chris	Puget Sound Energy
Carpenter, Matthew	
Cavoukian, Ann	Office of the Information and Privacy Commissioner of Ontario
Chan, Rida	Deloitte & Touche, LLP
Chaney, Mike	Securicon
Charbonneau, Sylvain	Hydro-Quebec
Chasko, Stephen	Landis+Gyr
Chason, Glen	EPRI
Chaudhry, Hina	Argonne National Labs
Chhabra, Rahul	Burns & McDonnell Engineering
Chibba, Michelle	Office of the Information and Privacy Commissioner of Ontario
Choubey, TN	Southern California Edison
Chow, Edward	U of Colorado at Colorado Springs
Chow, Richard	PARC
Chris Starr	General Dynamics
Christopher, Jason	FERC
Chudgar, Raj	Sungard
Chung, Raymond	National Technical Systems, Inc.
Churchill, Alex	Duke Energy
Cioni, Mark V.	MV Cioni Associates, Inc.
Clark, Jamie	OASIS
Claypoole, Ted	Womble Carlyle Sandridge & Rice, PLLC
Clements, Abraham	Sandia National Laboratories
Clements, Sam	Pacific Northwest National Laboratory
Cleveland, Frances	Xanthus Consulting International
Cohen, Michael	Mitre
Cohen, Yossi	
Collier, Albert	Alterium, LLC
Coney, Lillie	Electronic Privacy Information Center
Coomer, Mark	ITT Defense and Information Solutions
Coop, Mike	ThinkSmartGrid
Cornish, Kevin	Enspiria
Cortes, Sarah	Inman Technology IT

Cosio, George	Florida Power and Light
Cox, William	Cox Software Architects
Cragie, Robert	Jennic LTD
Crane, Melissa	Tennessee Valley Authority
Crljenica, Igor	State of Michigan
Cuen, Lita	LC RISQ & Associates
Cui, Stephen	Microchip Technology
Czaplewski, John	Northrup Grumman Corp.
Dagle, Jeff	Pacific Northwest National Laboratory
Dalva, Dave	Stroz Friedberg
Danahy, Jack	Bochman & Danahy Research
Danezis, George	Microsoft
Dangler, Jack	
Das, Subir	Applied Communication Sciences
Davis, Scott	Sensus
Davison, Brian	Public Utility Commission of Texas
De Petrillo, Nick	Industrial Defender
Delenela, Ann	Ercot
DeLoach, Tim	IBM Global Business Services
DePeppe, Doug	i2IS Cyberspace Solutions
di Sabato, Mark	
Dieffenbach, Dillon	Ernst & Young
Dienhart, Mary	Xcel Energy
Dierking, Tim	Aclara Power-Line Systems, Inc.
Dillon, Terry	APS
Dinges, Sharon	Trane
Dion, Thomas	Dept of Homeland Security
Do, Tam	Southwest Research Institute
Dodd, David	pbnetworks
Dodson, Greg	Dominion Resources Services, Inc.
Don-Arthur, George	Alterium LLC
Doreswamy, Rangan	Verisign, Inc.
Doring, Ernest	Pacific Gas & Electric
Dorn, John	Accenture
Dougherty, Steven	IBM
Downum, Wesley	Telcordia
Dransfield, Michael	National Security Agency

Drgon, Michele	DataProbity
Drozinski, Timothy	Florida Power & Light Company
Drummond, Rik	Drummond Group
Dubrawsky, Ido	Itron
Duffy, Paul	Cisco Systems
Duggan, Pat	ConEd
Dulaney, Mike	Arxan Technologies, Inc.
Dunfee, Rhonda	Department of Energy
Dunphy, Mary	
Dunton, Benjamin	NYS Department of Public Service
Dupper, Jeff	Ball Aerospace & Technologies
Duren, Michael	Protected Computing
Dutta, Prosenjit	Utilities AMI Practice
Earl, Frank	Earl Consulting
Eastham, Bryant	Panasonic Electric Works Laboratory of America (PEWLA)
Edgar, Tom	Pacific Northwest National Laboratory
Eggers, Matthew	U.S. Chamber of Commerce
Eigenhuis, Scott M	
Ellison, Mark	DTE Energy
Emelko, Glenn	ESCO
Engels, Mark	Dominion Resources Services, Inc.
Ennis, Greg	Wi-Fi Alliance
Enstrom, Mark	NeuStar
Eraker, Liz	Samuelson Clinic at UC Berkeley
Erickson, Dave	California Public Utility Commission
Ersue, Mehmet	Nokia Siemens Networks
Estefania, Maria	ATIS
Eswarahally, Shrinath	Infineon Technologies NA
Evans, Bob	Idaho National Laboratory
Ewing, Chris	Schweitzer Engineering Labs
Fabela, Ronnie	Lockheed Martin
Fabian, Michael	Wurldtech Security Technologies
Faith, Doug	MW Consulting
Faith, Nathan	American Electric Power
Famolari, David	Telcordia Technologies
Faure, Jean-Philippe	Progilon Co.

Fennell, Kevin	Landis+Gyr
Fenner, Philip	American Electric Power, Inc.
Fischer, Ted	Norwich University Applied Research Institutes (NUARI)
Fisher, Jim	Noblis
Fishman, Aryah	Edison Electric Institute
Fitzpatrick, Gerald	NIST
Flickinger, Derek	ThinkSmartGrid, LLC
Flowers, Tom	Control Center Solutions, LLC
Foglesong, Anna	Pacific Gas & Electric
Ford, Guy	New Hampshire Electric Cooperative
Foster, William	Lumi Wireless Technologies
Francis, Daniel	AEP
Franklin, Troy	FriiPwrLtd
Franz, Matthew	SAIC
Fraser, Barbara	Cisco
Fredebeil, Karlton	Tennessee Valley Authority
Frederick, Jennifer	Direct Energy
Fredrickson, Dan	Tendril Inc.
Freund, Mark	Pacific Gas and Electric Company
Friedman, Dan	
Frogner, Bjorn	
Fulford, Ed	
Fuloria, Shailendra	Cambridge University
Fulton, Joel	
Futch, Matt	IBM Energy and Utilities
Gailey, Mike	CSC
Galli, Stefano	ASSIA, Inc.
Garrard, Ken	Aunigma Network Solutions Corp.
Gassko, Irene	Florida Power & Light
Gaulding, Win	Northrop Grumman Information Systems
Gerber, Josh	San Diego Gas and Electric
Gerbino, Nick	Dominion Resources Services, Inc.
Gering, Kip	Itron
Gerney, Arkadi	OPOWER
Gerra, Arun	University of Colorado, Boulder
Ghansah, Isaac	California State University Sacramento

Gibbs, Derek	SmartSynch
Gilchrist, Grant	EnerNex
Gill, Jeff	RuggedCom Inc.
Gillmore, Matt	CMS Energy
Givens, Beth	Privacy Rights Clearinghouse
Glassey, Todd	Certichron Inc.
Glavin, Kevin	Cigital
Glenn, Bill	Westar Energy, Inc.
Goff, Ed	Progress Energy
Gokul, Jay	Technology Crest Corp.
Golla, Ramprasad	Grid Net
Gomez, Aaron	Drummond Group
Gonzalez, Efrain	Southern California Edison
Gooding, Jeff	Southern California Edison
Goodson, Paul	ISA
Gorog, Christopher	Atmel Corporation
Grainger, Steven	General Dynamics
Grazdina, Baiba	Duke Energy
Greenberg, Alan M.	
Greenfield, Neil	American Electric Power, Inc.
Greer, David	University of Tulsa
Griffin, Slade	Enernex
Grochow, Jerrold	MIT
Gulick, Jessica	SAIC
Gunter, Carl	U. of Illinois
Gupta, Rajesh	UC San Diego
Gupta, Sarbari	Electrosoft
Gutierrez, Julio	Florida Power & Light
Habre, Alex	PJM
Hague, David	
Halasz, Dave	Aclara
Halbgewachs, Ronald D.	Sandia National Laboratories
Hall, Tim	Mocana
Hallman, Georgia	Guidance Software
Hambrick, Gene	Carnegie Mellon University
Hanley, James	General Electric
Hardjono, Thomas	MIT

Harkins, Dan	Aruba Networks
Harper, John	American Electric Power, Inc.
Harris, Greg	Harris Corporation
Harris, Therese	Public Utility Commission of Texas
Harrison, Becky	GridWise Alliance
Hartman, Darren	ICSA Labs
Hartmann, Chad	Xcel Energy
Hashimoto, Mikio	Toshiba
Hastings, Nelson	NIST
Hawk, Carol	Department of Energy
Hayden, Ernest	Verizon
He, Donya	BAE Systems
Heger, Mary	Ameren Services
Heiden, Rick	Pitney Bowes
Heidner, Dennis	
Helm, Donny	Oncor
Henderson, Lynn	Northrop Grumman Information Systems
Hensel, Hank	CSC
Herold, Rebecca	Privacy Professor Rebecca Herold & Associates, LLC
Heron, George L.	BlueFin Security
Herrell, Jonas	University of California, Berkeley
Hertzler, Megan	Xcel Energy
Hertzog, Christine	Smart Grid Library
Hieta, Karin	California Public Utility Commission
Higgins, Moira	TSRI
Highfill, Darren	SCE
Hilber, Del	Constellation Energy
Histed, Jonathan	Novar | Honeywell
Hoag, John C.	Ohio University
Holland, Clayton	DHS / Missing Link Security
Hollenbaugh, Greg	Electrosoft Inc.
Holstein, Dennis	OPUS Consulting Group
Hoofnagle, Chris	University of California, Berkeley
Hooper, Emmanuel	Harvard University
Hornung, Lynette	
House, Joshua	Future of Privacy

Houseman, Doug	Capgemini Consulting
Howie, Sarah	NextEnergy Center
Huber, Robert	Critical Intelligence
Hudson, John	CenterPoint Energy
Hughes, Joe	EPRI
Humphrey, Robert	Duke Energy
Humphries, Scott	SmartSynch
Hunt, Chuck	
Hunteman, William	Department of Energy
Hurley, Jesse	Shift Research, LLC
Hussey, Laura	Schweitzer Engineering Laboratories, Inc.
Hutson, Jeff	Accenture
Huzmezan, Mihai	General Electric
Ibrahim, Erfan	EPRI
Iga, Yoichi	Renesas Electronics Corp.
Ilic, Jovan	
Ilic, Marija	Carnegie-Mellon University
Inaba, Atsushi	GlobalSign
Iorga, Michaela	NIST
Ivers, James	SEI
Jacobs, Leonard	Xcel Energy
Jaffray, Travis	
Jaokar, Ajit	Futuretext
Jarrett, Terry	Missouri Public Service Commission
Jeirath, Nakul	Southwest Research Institute
Jepson, Robert	Lockheed Martin Energy Solutions
Jin, Chunlian	Pacific Northwest National Laboratory
Joffe, Rodney	NeuStar
Johnson, Freemon	NIST
Johnson, Oliver	Tendril
Jones, Barry	Sempra
Jones, Derrick	Enteredge Technology, LLC
Jones, Derrick	Merlin International, Inc.
Joshi, Makarand	
Kahl, Steve	North Dakota
Kahn, Ely	FriiPwrLtd
Kaiser, Lisa	Department of Homeland Security

Kalbfleisch, Roderick	Northeast Utilities
Kanda, Mitsuru	Toshiba
Kashatus, Jennifer	Womble Carlyle Sandridge & Rice, PLLC
Kassakhian, Ken	Colorado Dept. of Regulatory Authorities
Kastner, Ryan	University of California at San Diego
Katz, Martha Lessman	Gordon, Feinblatt, Rothman, Hoffberger & Hollander, LLC
Kaufman, David R.	Honeywell International
Kavanagh, Mike	Constellation Energy
Kellogg, Shannon	EMC
Kelly, Lee	
Kenchington, Henry	U.S. Department of Energy
Kenney, Charlie	IBM
Kerber, Jennifer	Tech America
Khera, Rohit	S & C Electric Company
Khurana, Himanshu	Honeywell
Kiely, Sarah	NRECA
Kilbourne, Brett	Utilities Telecom Council
Kim, Jin	Risk Management Consulting, CRA International
Kim, Tae-Wan	NIST
Kimura, Randy	General Electric
King, Charlie	BAE Systems
Kirby, Bill	Aunigma Network Solutions Corp.
Kiss, Gabor	Telcordia
Kladko, Stan	Aspect Labs
Klein, Stanley A.	Open Secure Energy Control Systems, LLC
Klerer, Mark	
Kobayashi, Nobuhiro	Mitsubishi Electric
Kobes, Jason	Northrop Grumman Corp.
Koliwad, Ajay	General Electric
Kotting, Chris	ThinkSmartGrid, LLC
Koyuncu, Osman	Texas Instruments, Inc.
Kravitz, David	
Krishna, Karthik	Michigan Technological University
Krishnamurthy, Hema	ITT Information Assurance
Kube, Nate	Wurldtech
Kulkarni, Manoj	Mocana

Kursawe, Klaus	
Kuruganti, Phani Teja	EMC2
Kyle, Martin	Sierra Systems
Lackey, Kevin	Electric Reliability Council of Texas (ERCOT)
Lakshminarayanan, Sitaraman	General Electric
LaMarre, Mike	Austin Energy ITT
Lane, Anne	American Electric Power, Inc.
LaPorte, TJ	Landis+Gyr
Larsen, Harmony	Infogard
Lauriat, Nicholas A.	Network and Security Technologies
LaVoy, Lanse	DTE Energy
Lawrence, Bill	Lockheed Martin Corporation
Lawson, Barry	NRECA
Lebanidze, Evgeny	Cigital
Leduc, Jean	Hydro-Quebec
Lee, Annabelle	EPRI
Lee, Cheolwon	Electronics and Telecommunications Research Institute
Lee, Gunhee	Electronics and Telecommunications Research Institute
Lee, JJ	LS Industrial Systems
Lee, Travis	SMUD
Lee, Virginia	eComp Consultants
Legary, Michael	Seccuris, Inc.
Leggin, Nick	West Monroe
Lenane, Brian	SRA International
Leuck, Jason	Lockheed Martin Corporation
Levinson, Alex	Lockheed Martin Information Systems and Global Solutions
Levy, Roger	Lawrence Berkeley National Laboratory
Lewis, David	Hydro One
Lewis, Rob	Trustifiers Inc.
Li, Tony	CLP Power Hong Kong Lmtd
Libous, Jim	Lockheed Martin Systems Integration – Owego
Light, Matthew	NERC
Lilley, John	Sempra
Lima, Claudio	Sonoma Innovation
Lin, Yow-Jian	Telcordia Technologies

Lintzen, Johannes	Utimaco Safeware AG
Lipson, Howard	CERT, Software Engineering Institute
Locke, David	Verizon
Loomis, Joe	Southwest Research Institute
Lowe, Justin	PA Consulting Group
Lynch, Jennifer	University of California, Berkeley
Machado, Raphael	Inmetro – Instituto Nacional de Metrologia, Brazil
Maciel, Greg	Uniloc USA
Madden, Jason	MRIGlobal
Magda, Wally	Industrial Defender
Magnuson, Gail	
Mahmud, Shamun	DLT Solutions, Incorporated
Malashenko, Liza	California PUC
Malina, Alfred	SG-CG Smart Grid Information Security WG
Manjrekar, Madhav	Siemens
Manucharyan, Hovanes	LinkGard Systems
Maria, Art	AT&T
Markham, Tom	Honeywell
Marks, Larry	
Martin, Gordon	Alabama Power
Martinez, Catherine	DTE Energy
Martinez, Ralph	BAE Systems
Marty, David	University of California, Berkeley
Masch, Brian	Ernest & Young
Mashima, Daisuke	Fujitsu Lab of America
McBride, Sean	Critical Intelligence
McCaffree, Matt	OPOWER
McComber, Robert	Telvent
McCullough, Jeff	Elster Group
McDonald, Jeremy	Southern California Edison
McGinnis, Douglas	Exelon
McGrew, David	Cisco
McGuire, John	American Electric Power, Inc.
McGurk, Sean	Dept of Homeland Security
McKay, Brian	Booz Allen Hamilton
McKenna, Erin	
McKinnon, David	Pacific Northwest National Laboratory

McMahon, Liam	Bridge Energy Group
McMillin, Bruce	Missouri University of Science and Technology
McNay, Heather	Landis+Gyr
McQuade, Rae	NAESB
Medlar, Arthur	LocalPower
Melton, Ron	Pacific Northwest National Laboratory
Mennella, Jean-Pierre	SG-CG Smart Grid Information Security WG
Mertz, Michael	Southern California Edison
Metke, Tony	Motorola
Michail, David	Zuber & Taillieu LLP
Milbrand, Doug	Concurrent Technologies Corporation
Millard, David	Georgia Tech Research Institute
Miller, Joel	Merrion Group
Miller, Melvin	Nulink Wireless
Mirza, Wasi	Motorola
Mitsuru, Kanda	Toshiba
Mitton, David	Ambient Corp.
Modeste, Ken	Underwriters Laboratories, Inc.
Mohan, Apurva	Honeywell
Moise, Avy	Future DOS R&D Inc.
Molina, Jesus	Fujitsu Ltd.
Molitor, Paul	NEMA
Mollenkopf, Jim	CURRENT Group
Moniz, Paulo	
Monkman, Brian	ICSA Labs
Montgomery, Jason	American Electric Power, Inc.
Moody, Diane	American Public Power Association
Morese, Alex	State of Michigan
Morris, Tommy	Mississippi State University
Mosely, Donald	FriiPwrLtd
Moskowitz, Robert	ICSAlabs
Mulberry, Karen	Neustar
Munoz, Tony	Colorado Department of Regulatory Agencies
Nahas, John	ICF International
Nakamura, Masafumi	Mitsubishi Research Institute, Inc.
Navid, Nivad	Midwest ISO
Neergaard, Dude	Oak Ridge National Laboratory

Newhouse, Bill	NIST
Nguyen, Nhut	Samsung
Nidetz, Lee	TSRI
Nissim, Sharon Goott	Electronic Privacy Information Center
Noel, Paul	ASI
Norton, Dave	Entergy
Nutaro, James J.	Southern California Edison
O'Neill, Ivan	Southern California Edison
O'Sullivan, Mairtin	
Obregon, Eduardo	University of Texas at El Paso
Oduyemi, Felix	Southern California Edison
Ohba, Yoshihiro	Toshiba
Okunami, Peter M.	Hawaiian Electric Company, Inc.
Old, Robert	Siemens Building Technologies, Inc.
Oldak, Mike	Utilities Telecom Council
Olive, Kay	Olive Strategies
Ornelas, Efrain	PG&E
Overman, Thomas M.	Boeing
Owens, Andy	Plexus Research
Owens, Leslie	American Systems
Pabian, Michael	Exelon Legal Services
Pace, James	Silver Spring Networks
Pahl, Chris	Southern California Edison Company
Paine, Tony	Kepware Technologies
Pal, Partha	Raytheon BBN Technologies
Pales, Wayne	CLP Power Hong Kong Lmtd
Palmquist, Scott	Itron
Papa, Mauricio	University of Tulsa
Parthasarathy, Jagan	Business Integra
Patel, Chris	EMC Technology Alliances
Pearce, Thomas C. II	Public Utilities Commission of Ohio
Pederson, Perry	U.S. Nuclear Regulatory Commission
Peralta, Rene	NIST
Peters, Mike	FERC
Peterson, Thomas	Boeing
Phillips, Matthew	Electronic Privacy Information Center
Phillips, Michael	Centerpoint Energy

Phinney, Tom	
Phiri, Lindani	Elster Group
Pillitteri, Victoria Yan	NIST
Pittman, James	Idaho Power
Pittman, Jason	DTE Energy
Planter-Pascal, Claudine	FERC
Polonetsky, Jules	The Future of Privacy Forum
Polulyakh, Diana	Advanced Data Security
Polulyakh, Eugene	Advanced Data Security
Pope, John	NeuStar
Porterfield, Keith	Georgia System Operations Corporation
Potter, Rick	Alliant Energy
Powell, Terry	L-3 Communications
Proctor, Brian	Sempra Energy Utilities
Prowell, Stacy	Oak Ridge National Laboratory
Puri, Anuj	IEEE
Pyle, Mike	Schneider Electric
Pyles, Ward	Southern Company
Qin, Andy	Cisco
Qin, Jason	Skywise Systems
Qiu, Bin	E:SO Global
Quinn, Steve	Sophos
Rader, Bodhi	FERC
Radgowski, John	Dominion Resources Services, Inc
Ragsdale, Gary L.	Southwest Research Institute
Raines, Tim	Black Hills, Corp.
Rakaczky, Ernest A.	Invensys Global Development
Rao, Josyula R	IBM
Ray, Indrakshi	Colorado State University
Reddi, Ramesh	Intell Energy
Reed, Rebecca	Texas PUC
Revill, David	Georgia Transmission Corp.
Rhéaume, Réjean	Hydro-Quebec
Richtsmeier, Dorann	Northrup Grumman Corp.
Rick Schantz	BBN
Riepenkroger, Karen	Sprint
Ristaino, Andre	

Rivaldo, Alan	Public Utility Commission of Texas
Rivero, Al	Telvent
Roberts, Don	Southern Company Transmission
Roberts, Jeremy	LonMark International
Robinson, Brandon	Balch & Bingham LLP
Robinson, Charley	International Society of Automation
Robinson, Eric	ITRON
Robinson, Louis	Constellation Energy
Rodriguez, Gene	IBM
Rothke, Ben	National Grid
Ruano, Julio	IBM
Rueangvivatanakij, Birdie	Missing Link Security
Rumery, Brad	Sempra
Rush, Bill	
Russell, Dave	Noveda Technologies
Rutfield, Craig	NTRU Cryptosystems, Inc.
Rutkowska, Joanna	Invisible Things
Rutkowski, Tony	Yaana Technologies
Sachs, Marcus	Verizon Communications
Sacre, Spiro	National Technical Systems, Inc.
Saint, Bob	National Rural Electric Cooperative Association
Sakane, Hiro	NIST
Sakr, Osman	National Technical Systems, Inc.
Salons, Deborah	
Sambasivan, Sam	AT&T
Sanders, William	University of Illinois
Saperia, Jon	
Sargent, Robert	Cisco Systems, Inc.
Saunders, Scott	SMUD
Scace, Caroline	NIST
Schaefer, Krystina	Ohio PUC
Schantz, Rick	Raytheon BBN Technologies
Scheff, Andrew	Scheff Associates
Schmitt, Laurent	SG-CG Smart Grid Information Security WG
Schneider, Brandon	SRA International
Schneider, Don	Duke Energy
Schoechle, Timothy	

Schomburg, Paul	Panasonic Corp. of North America
Schooler, Eve	Intel Labs
Schroeder, Joel	Inmarsat Inc.
Schulman, Ross	Center for Democracy and Technology
Schultz, Bill	Vanderbilt University
Schwarz, David	Department of Homeland Security
Sciacca, Sam	SCS Consulting, LLC
Sconzo, Mike	Electric Reliability Council of Texas
Scott, David	Accenture
Scott, Kat	EPIC
Scott, Richard	
Scott, Tom	Progress Energy
Searfoorce, Daniel	Pennsylvania Public Utility Commission
Searle, Justin	UtiliSec
Seewald, Mike	Cisco
Seo, Jeongtaek	Electronics and Telecommunications Research Institute
Sequino, David	Green Hills Software
Shah, Nihar	Information Law Group
Shakespeare, Jared	Western Electricity Coordinating Council
Shastri, Viji	MCAP Systems
Shavit, Juliet	SmartMark Communications, LLC
Shaw, Vishant	Enernex
Shein, Robert	EDS
Sheldon, Rick	Oakridge National Laboratory
Sherman, Sean	Triton
Shetty, Ram	General Electric
Shin, Mark	Infogard
Shipley, AJ	Wind River
Shorter, Scott	Electrosoft
Shpantzer, Gal	
Silverstone, Ariel	
Sinai, Nick	Federal Communications Commission
Singer, Bryan	Kenexis
Sisley, Elizabeth	University of Minnesota
Sitbon, Pascal	EDF Inc.
Skare, Paul	Pacific Northwest National Laboratory

Skidmore, Charlotte	Association of Home Appliance Manufacturers
Slack, Phil	Florida Power & Light Company
Smith, Brian	EnerNex
Smith, Charles	General Electric
Smith, Rhett	Schweitzer Engineering Laboratories, Inc.
Smith, Ron	ESCO Technologies Inc.
Smith, Zane	FriiPwrLtd
Sokker, Anan	Florida Power & Light Company
Sood, Kapil	Intel Labs
Sorebo, Gilbert	SAIC
Soriano, Erick	Garvey Schubert Barer
Souza, Bill	
Spirakis, Charles	Google
St Johns, Michael	Nth Permutation
Staggs, Kevin	Honeywell
Stallings, Amanda	Public Utility Commission of Ohio
Stammberger, Kurt	Mocana
Standifur, Thomas	KEMA Inc.
Starr, Christopher	General Dynamics Advanced Information Systems
Steiner, Michael	IBM Thomas J. Watson Research Center
Stepanovich, Amie	EPIC
Sterling, Joyce	NitroSecurity
Stevens, James	Software Engineering Institute
Stewart, Clinton	
Stitzel, Jon	Burns & McDonnell Engineering Company, Inc.
StJohns, Michael	Nth Permutation
Storey, Clay	Avista Corp.
Stouffer, Keith	NIST
Strickland, Tom	General Electric
Struik, Rene	Struik Security Consultancy
Struthers, Brent	NeuStar
Stuber, Micheal	Itron
Sturek, Don	Grid2Home
Sturm, John	Indiana State University
Stycos, Dave	Zocalo Data Systems, Ltd.
Suarez, Luis Tony	Tennessee Valley Authority
Suchman, Bonnie	Troutman Sanders LLP

Sullivan, Kevin	Microsoft
Sung, Lee	Fujitsu
Sushilendra, Madhava	EPRI
Swanson, Marianne	NIST
Sweet, Jeffrey	American Electric Power, Inc.
Tallent, Michael	Tennessee Valley Authority
Taylor, Dave	Siemens
Taylor, Malcolm	Carnegie Mellon University
Tengdin, John	OPUS Consulting
Thanos, Daniel	General Electric
Thaw, David	Hogan & Hartson
Thomas, Sarah	California Public Utility Commission
Thomassen, Tom	Symantec
Thompson, Catherine	Information and Privacy Commissioner's Office of Ontario
Thompson, Daryl L.	Thompson Network Consulting
Thompson, Mark	Aclara RF Systems, Inc.
Thomson, Matt	General Electric
Thrasher, Shelly	Office of the Information & Privacy Commissioner of Ontario
Tien, Lee	Electronic Freedom Foundation
Tiffany, Eric	Liberty Alliance
Tillman, Leonard	Balch & Bingham LLP
Tobin, Tim	Hogan Lovells US LLP
Toecker, Michael	Burns & McDonnell
Tolway, Rich	APS
Tom, Steve	Idaho National Laboratory
Tran, Lan	Tangible
Trapp, Bob	Booz Allen Hamilton
Trayer, Mark	Samsung
Trimble, Curtis D.	
Truskowski, Mike	Cisco System, Inc.
Tull, Laurie	Anakam, an Equifax Company
Tunney, Carrin	DTE Energy
Turgeon, Anyck	
Turke, Andy	Siemens Energy, Inc.
Turner, Patrick	Secure Works

Turner, Steve	International Broadband Electric Communications, Inc.
Uhrig, Rick	Electrosoft
Urban, Jennifer	Samuelson Clinic at UC Berkeley
Uzhunnan, Abdul	DTE Energy
Vader, Rob	DTE Energy
van Loon, Marcel	AuthenTec
Vankayala, Vidya	Cisco
Vayos, Daphne	Northeast Utilities
Veillette, Michel	Trilliant Inc.
Veltsos, Christophe	Minnesota State University
Venkatachalam, R. S.	Mansai Corporation
Vettoretti, Paul	SBC Global
Villarreal, Christopher	California Public Utilities Commission
Voje, Joe	Snohomish County PUD
Vollebregt, Paul	MobiComm Communications
Wacks, Kenneth P.	GridWise Architecture Council
Waddell, Dan	Tantus Tech
Waheed, Aamir	Cisco Systems, Inc.
Walia, Harpreet	Wave Strong Inc.
Wall, Perrin	CenterPoint Energy
Wallace, Donald	Itron
Walsh, Jack	ICSA Labs
Walters, Keith	Edison Electric Institute
Walters, Ryan	COO TerraWi Communications
Wang, Alex	Cisco Systems, Inc.
Wang, Longhao	Samuelson Clinic at UC Berkeley
Wang, Yongge	University of North Carolina-Charlotte
Ward, Mark	Pacific Gas & Electric Company
Warner, Christopher	Pacific Gas & Electric Company
Watson, Brett	NeuStar
Webb, Kyle	Deloitte & Touche LLP
Weber, Don	InGuardians
Wei, Dong	SIEMENS Corporation
Weimerskirch, Andre	Escrypt
Wepman, Joshua	SAIC Commercial Business Services
West, Andrew C	Invensys Process Systems

West, Troy	Cleco Corpo.
Weyer, John A.	John A. Weyer and Associates
Whitaker, Kari	LockDown, Inc.
White, Jim	Uniloc USA, Inc.
Whitney, Tobias	The Structure Group
Whitsitt, Jack	
Whyte, William	Ntru Cryptosystems, Inc.
Wiese, Sean	National Information Solutions Cooperative
Williams, Jeffrey	
Williams, Terron	Elster Electricity
Wilson, Chris	TechAmerica
Wilson, Jason	Duke Energy
Wingo, Harry	Google
Witnov, Shane	University of California, Berkeley
Wohnig, Ernest	System 1, Inc.
Wolf, Dana	RSA
Wollman, David	NIST
Worden, Michael	New York State Public Service Commission
Worthington, Charles	Federal Communications Commission
Wright, Andrew	N-Dimension Solutions
Wright, Christine	Texas PUC
Wright, Josh	Inguardians
Wu, Lei	Clarkson University
Wu, Richard	Nokia Siemens Networks, USA
Wyatt, Michael	ITT Advanced Technologies
Xia, Sharon	ALSTOM Grid Inc.
Yakobitis, John J.	Federal Energy Regulatory Commission
Yao, Taketsugu	Oki Electric Industry, Co., Ltd
Yap, Xiang Ling	MIT
Yardley, Tim	University of Illinois
Yodaiken, Ruth	Federal Trade Commission
Yoo, Kevin	Wurldtech
Zausner, Alan	
Zummo, Paul	American Public Power Association
Zurcher, John	SRA