
The Smart Grid Interoperability Panel – Cyber Security Working Group

July 2010
REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

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

National Institute of Standards and Technology Interagency Report 7628:
Vol. 1, Smart Grid Cyber Security Strategy
89 pages (July 2010)

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

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

Additional thanks are extended to Diana Johnson (Boeing) for serving as a senior technical editor for this report. Her expertise, patience, and dedication were critical in producing a quality report. Thanks are extended to Vicky Yan (BAH). Her enthusiasm and willingness to jump in with both feet are really appreciated.

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

Figure 1-1 Tasks in the Smart Grid Cyber Security Strategy ........................................................... 7
Figure 3-1 Power Usage to Personal Activity Mapping ................................................................. 27
Figure 3-2 NIST Conceptual Model ..............................................................................................29

LIST OF TABLES

Table 1-1 Categories of Adversaries to Information Systems .......................................................... 9
Table 3-1 Information potentially available through the Smart Grid ............................................. 40
Table 3-2 Potential Privacy Concerns and Descriptions................................................................. 41
Table 3-3 Potential Privacy Impacts that Arise from the Collection and Use of Smart
Grid Data........................................................................................................... 44
OVERVIEW AND REPORT ORGANIZATION

REPORT OVERVIEW

Version 1.0 (V1.0) of NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, is the Smart Grid Interoperability Panel—Cyber Security Working Group’s (SGIP-CSWG’s) report for individuals and organizations who will be addressing cyber security for Smart Grid systems. This includes, for example, vendors, manufacturers, utilities, system operators, researchers, and network specialists; and individuals and organizations representing the IT, telecommunications, and electric sectors. Individuals reading this report are expected to have a basic knowledge of the electric sector and a basic understanding of cyber security.

AUDIENCE

This report is intended for a variety of organizations that may have overlapping and different perspectives and objectives for the Smart Grid. For example—

- **Utilities/asset owners/service providers** may use this report as guidance for a specific Smart Grid information system implementation;
- **Industry/Smart Grid vendors** may base product design and development, and implementation techniques on the guidance included in this report;
- **Academia** may identify research and development topics based on gaps in technical areas related to the functional, reliability, security, and scalability requirements of the Smart Grid;
- **Regulators/policy makers** may use this report as guidance to inform decisions and positions, ensuring that they are aligned with appropriate power system and cyber security needs.

This report is divided into three volumes.

- **Volume 1** and appendixes provide an overview of the cyber security strategy for the Smart Grid and a discussion of privacy and the Smart Grid. This volume is intended for individuals who want a high level summary of the work performed by the CSWG and the various subgroups of the CSWG.
- **Volume 2** and appendixes include the logical reference architecture and the high level security requirements. This volume is intended to be used as a guideline for individuals and organizations as they design, develop, implement and maintain the Smart Grid information systems.
- **Volume 3** and appendixes include the detailed analyses used to select and modify the security requirements included in Volume 2. Volume 3 also includes specific information that may be used by an organization’s technical staff as they assess and configure Smart Grid information systems.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Cyber Security Strategy
Chapter 1 – Cyber Security Strategy includes background information on the Smart Grid and the importance of cyber security in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the cyber security strategy for the Smart Grid and the specific tasks within this strategy.

Chapter 2 – High Level Logical Architecture includes a diagram that depicts a composite high level view of the actors within each of the Smart Grid domains.

Chapter 3 – Privacy and the Smart Grid includes a privacy impact assessment for the Smart Grid with a discussion of mitigating factors. The chapter also identifies potential privacy issues with the new capabilities included in the Smart Grid.

Appendix A – State Laws – Smart Grid and Electricity Delivery
Appendix B – Privacy Use Cases
Appendix C – Privacy Related Definitions

Volume 2 – Security Architecture and Security Requirements

Chapter 4 – Logical Security Architecture 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 proposed Smart Grid.

Chapter 5 – 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 4.

Chapter 6 – 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 D – Crosswalk of Cyber Security Documents
Appendix E – Example Security Technologies and Procedures to Meet the High Level Security Requirements

Volume 3 – Supportive Analyses and References

Chapter 7 – Vulnerability Classes includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.

Chapter 8 – Bottom-Up Security Analysis of the Smart Grid identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.

Chapter 9 – Research and Development Themes for Cyber Security in the Smart Grid includes R&D themes that identify where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid.

Chapter 10 – 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 11 – *Key Power System Use Cases for Security Requirements* identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.
- Appendix F – *Logical Architecture and Interfaces of the Smart Grid*
- Appendix G – *Analysis Matrix of Interface Categories*
- Appendix H – *Mappings to the High Level Security Requirements*
- Appendix I – *Glossary and Acronyms*
- Appendix J – *SGIP-CSWG Membership*
EXECUTIVE SUMMARY

Smart Grid technologies will introduce millions of new intelligent components to the electric grid that communicate in much more advanced ways (two-way communications, dynamic optimization, and wired and wireless communications) than in the past. Two areas are of critical importance in “getting it right”—cyber security and privacy. Development of the Guidelines for Smart Grid Cyber Security began with the establishment of a Cyber Security Coordination Task Group (CSCTG) led by the National Institute of Standards and Technology (NIST). The CSCTG now numbers more than 450 participants from the private sector (including vendors and service providers), manufacturers, various standards organizations, academia, regulatory organizations, and federal agencies. This group has been renamed under the Smart Grid Interoperability Panel (SGIP) as the Cyber Security Working Group (SGIP-CSWG). Cyber security is being addressed using a thorough process that results in a comprehensive set of cyber security requirements. As explained more fully in the first chapter of this report, these requirements were developed using a high-level risk assessment process that is defined in the cyber security strategy for the Smart Grid. Cyber security requirements are implicitly recognized as critical in all of the priority action plans discussed in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST Special Publication (SP) 1108) published in January 2010.

CYBER SECURITY STRATEGY FOR THE SMART GRID

The overall cyber security strategy for the Smart Grid examines both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The cyber security strategy needs to address prevention, detection, response, and recovery.

Implementation of a cyber security strategy requires the definition and implementation of an overall cyber security risk assessment process for the Smart Grid. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. This type of risk is one component of organizational risk, which can include many types of risk (e.g., investment, budgetary, program management, legal liability, safety, and inventory risk, as well as the risk from information systems). Because the Smart Grid includes systems from the information technology (IT), telecommunications, and energy sectors, the risk assessment process is applied to all three sectors as they interact in the Smart Grid. The information included in this report is guidance for organizations. NIST is not prescribing particular solutions through the guidance contained in this report. Each organization must develop its own cyber security strategy (including a risk assessment methodology) for the Smart Grid.

The security requirements and the supporting analyses that are 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 a Smart Grid information system. This report is neither a requirements document nor a checklist for what constitutes effective cyber security. Rather it focuses on specifying an analytical framework that may be useful to an organization. Each organization

---

must develop its own cyber security strategy for the Smart Grid. The information in this report serves as guidance to the various organizations for assessing risk and selecting appropriate security requirements.

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

The “Smart Grid Cyber Security Strategy” diagram outlines the strategic analysis tasks that are defined in the breakdown following the illustration.

![Smart Grid Cyber Security Strategy Diagram]

**Smart Grid Cyber Security Strategy**

**Task 1. Selection of use cases with cyber security considerations.**

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

---

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

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

As with any assessment, a realistic analysis of the threats of inadvertent errors, acts of nature, and malicious threats is critical to the overall outcome. The Smart Grid is no different. It is recommended that all organizations take a realistic view of the threats and work with authorities, as needed, to glean the required information, which, it is anticipated, no single utility or other Smart Grid participant would be able to assess on their own. The following table summarizes the categories of adversaries to information systems. These adversaries need to be considered when performing a risk assessment for a Smart Grid information system.

### Categories of Adversaries to Information Systems

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation States</td>
<td>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.</td>
</tr>
<tr>
<td>Hackers</td>
<td>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.</td>
</tr>
<tr>
<td>Terrorists/ Cyberterrorists</td>
<td>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.</td>
</tr>
<tr>
<td>Organized Crime</td>
<td>Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.</td>
</tr>
<tr>
<td>Other Criminal Elements</td>
<td>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.</td>
</tr>
<tr>
<td>Industrial Competitors</td>
<td>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.</td>
</tr>
<tr>
<td>Disgruntled Employees</td>
<td>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.</td>
</tr>
<tr>
<td>Careless or Poorly Trained Employees</td>
<td>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.</td>
</tr>
</tbody>
</table>

A realistic assessment of threats and their applicability to subsequent risk-mitigation strategies is critical to the overall security of the Smart Grid.

Task 3. Specification of high level security requirements.

There are many requirements documents that may be applicable to the Smart Grid. Currently, only NERC Critical Infrastructure Protection (CIP) standards are mandatory for the bulk electric
system. The CSWG used three source documents for the cyber security requirements in this report—

- NERC CIP 002, 003-009, version 3
- NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009

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 maps the Smart Grid security requirements in this report to the security requirements in SP 800-53, The DHS Catalog, and the NERC CIPs. Each requirement falls in one of three categories: governance, risk and compliance (GRC); common technical, and unique technical. The GRC requirements are typically implemented at the organization level and augmented, as required, for specific Smart Grid information systems. The common technical requirements are applicable to all the Smart Grid information systems. The unique technical requirements are allocated to one or more of the logical interface categories. The 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.

**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.

**Task 4a. Development of a logical reference model.**

The SGIP-CSWG developed a more granular logical reference model for the Smart Grid using the NIST conceptual model and the use case diagrams developed at the various NIST Smart Grid workshops. This logical reference model consolidates the individual diagrams into a single diagram and expands upon the conceptual model. The logical reference model identifies logical interfaces between actors.

**Task 4b. Assessment of Smart Grid standards.**

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

---

3 NIST SP 800-53 is mandatory for federal agencies and the NERC CIPs are mandatory for the Bulk Power System. This NISTIR is a guidance document intended to be used as a baseline, and is not a mandatory standard.
Task 5. Conformity Assessment.

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

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

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

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 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 that could introduce new vulnerabilities;

---


Denial of electric service; and
Potential for compromise of data confidentiality, including the breach of customer privacy.

With the ongoing transition to the Smart Grid, the IT and telecommunication sectors will be more directly involved. These sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in their systems. These same vulnerabilities need to be assessed in the context of the Smart Grid infrastructure. In addition, the Smart Grid will have additional vulnerabilities due not only to its complexity, but also because of its large number of stakeholders and highly time-sensitive operational requirements.

In its broadest sense, cyber security for the power industry covers all issues involving automation and communications that affect the operation of electric power systems and the functioning of the utilities that manage them and the business processes that support the customer base. In the power industry, the focus has been on implementing equipment that can improve power system reliability. Until recently, communications and IT equipment were typically seen as supporting power system reliability. However, increasingly these sectors are becoming more critical to the reliability of the power system. For example, in the August 14, 2003 blackout, a contributing factor was issues with communications latency in control systems. With the exception of the initial power equipment problems, the ongoing and cascading failures were primarily due to problems in providing the right information to the right individuals within the right time period. Also, the IT infrastructure failures were not due to any terrorist or Internet hacker attack; the failures were caused by inadvertent events—mistakes, lack of key alarms, and poor design. Therefore, inadvertent compromises must also be addressed, and the focus must be an all-hazards approach.

NIST leads a Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP-CSWG) which now has more than 450 volunteer members from the public and private sectors, manufacturers, various standards organizations, academia, regulatory organizations, and federal agencies. Cyber security is being addressed using a thorough process that results in a comprehensive set of cyber security requirements. As explained more fully later in this chapter, these requirements were developed (or augmented, where standards/guidelines already exist) using a high-level risk assessment process that is defined in the cyber security strategy section of this report. Cyber security requirements are implicitly recognized as critical in all of the priority action plans discussed in the Special Publication (SP), *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0 (NIST SP 1108), which was published in January 2010.8 The CSWG has liaisons to other Smart Grid industry groups to support and encourage coordination among the various efforts. The documented liaisons are listed at http://collaborate.nist.gov/twiki-sggrdi/bin/view/SmartGrid/CSWGLiaisonInformation.

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

---

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

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

1.1 Cyber Security and the Electric Sector

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

Section 1301 of the Energy Independence and Security Act of 2007 (P.L. 110-140) states:

It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

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

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

The DOE Energy Sector-Specific Plan[9] “envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government.”

1.2 Scope and Definitions

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

Cyber Infrastructure: Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that

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

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

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

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

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

This report provides background information on the analysis process used to select and modify the security requirements applicable to the Smart Grid. The process includes both top-down and bottom-up approaches in the selection and modification of security requirements for the Smart Grid. The bottom-up approach focuses on identifying vulnerability classes, for example, buffer overflow and protocol errors. The top-down approach focuses on defining components/domains of the Smart Grid system and the logical interfaces between these components/domains. To reduce the complexity, the logical interfaces are organized into logical interface categories. The inter-component/domain security requirements are specified for these logical interface categories based on the interactions between the components and domains. For example, for the Advanced Metering Infrastructure (AMI) system, some of the security requirements are authentication of the meter to the collector, confidentiality for privacy protection, and integrity for firmware updates.

Finally, this report focuses on Smart Grid operations and not on enterprise operations. However, organizations should capitalize on existing enterprise infrastructures, technologies, support and operational aspects when designing, developing and deploying Smart Grid information systems.
1.3 SMART GRID CYBER SECURITY STRATEGY

The overall cyber security strategy for the Smart Grid examines both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The cyber security strategy needs to address prevention, detection, response, and recovery.

Implementation of a cyber security strategy requires the definition and implementation of an overall cyber security risk assessment process for the Smart Grid. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. This type of risk is one component of organizational risk, 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 energy sectors, the risk assessment process is applied to all three sectors as they interact in the Smart Grid. The information included in this report is guidance for organizations. NIST is not prescribing particular solutions through the guidance contained in this report. Each organization must develop its own cyber security strategy (including a risk assessment methodology) for the Smart Grid.

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

- The IT, telecommunications, and energy sector-specific plans (SSPs), initially published in 2007 and updated annually;
The next step in the Smart Grid cyber security strategy is to select and modify (as necessary) the security requirements. The documents used in this step are listed under the description for Task 3. This report aims to provide guidance for the electric sector as it addresses cyber security needs of the evolving Smart Grid and is neither a requirements document nor a checklist for what constitutes effective cyber security. Rather this report focuses on specifying an analytical framework, with cross-references to potentially useful standards and best practices that may be useful to an organization.

The security requirements and the supporting analyses included in this report may be used by strategists, designers, implementers, and operators of the Smart Grid (e.g., utilities, equipment manufacturers, regulators) as input to their risk assessment process and other tasks in the security lifecycle of the Smart Grid. The information serves as guidance to the various organizations for assessing risk and selecting appropriate security requirements. NIST is not prescribing particular solutions to cyber security issues through the guidance contained in this report. Each organization must develop its own cyber security strategy for the Smart Grid.

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

The tasks within the cyber security strategy for the Smart Grid are undertaken by participants in the SGIP-CSWG\(^\text{10}\). The remainder of this subsection describes the tasks that are being performed in the implementation of the cyber security strategy. Also included are the deliverables for each task. Because of the time frame within which this report was developed, the tasks listed on the following pages have been performed in parallel, with significant interactions among the groups addressing the tasks.

Figure 1-1 illustrates the tasks defined for the Smart Grid cyber security strategy. The tasks are defined following the figure.

---

10 The SGIP-CSWG was formerly known as the Cyber Security Coordination Task Group (CSCTG). The Cyber Security Working Group (CSWG) was established as a permanent working group within the Smart Grid Interoperability Panel (SGIP).
Task 1. Selection of use cases with cyber security considerations.\textsuperscript{11}

The use cases included in Appendix B 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 will be the basis for the selection of security requirements and the identification of gaps in guidance and standards related to the security requirements.

\textsuperscript{11} A use case is a method of documenting applications and processes for purposes of defining requirements.
**Vulnerability classes:** The initial list of vulnerability classes\(^\text{12}\) was developed using information from several existing documents and Web sites, e.g., NIST SP 800-82, Common Weakness Enumeration (CWE) vulnerabilities, and the Open Web Application Security Project (OWASP) vulnerabilities list. These vulnerability classes will ensure that the security controls address the identified vulnerabilities. The vulnerability classes may also be used by Smart Grid implementers, e.g., vendors and utilities, in assessing their systems. The vulnerability classes are included in chapter 7 of this report.

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

**Bottom-up analysis:** The bottom-up approach focuses on well-understood problems that need to be addressed, such as authenticating and authorizing users to substation intelligent electronic devices (IEDs), key management for meters, and intrusion detection for power equipment. Also, interdependencies among Smart Grid domains/systems were considered when evaluating the impacts of a cyber security incident. An incident in one infrastructure can potentially cascade to failures in other domains/systems. The bottom-up analysis is included in chapter 8 of this report.

**Top-down analysis:** In the top-down approach, logical interface diagrams were developed for the six functional priority areas that were the focus of the initial draft of 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., immature or proprietary protocols, insecure locations, integrity requirements) was defined and the attributes allocated to the interface categories, as appropriate. This logical interface category/attributes matrix is used in assessing the impact of a security compromise on confidentiality, integrity, and availability. The level of impact is denoted as low, moderate, or high.\(^\text{13}\) 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.

---

\(^{12}\) 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.

\(^{13}\) The definitions of low, moderate, and high impact are found in [FIPS 199](https://csrc.nist.gov/resources/publications/fips-documents).
Table 1-1 Categories of Adversaries to Information Systems

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation States</td>
<td>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.</td>
</tr>
<tr>
<td>Hackers</td>
<td>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.</td>
</tr>
<tr>
<td>Terrorists/ Cyberterrorists</td>
<td>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.</td>
</tr>
<tr>
<td>Organized Crime</td>
<td>Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.</td>
</tr>
<tr>
<td>Other Criminal Elements</td>
<td>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.</td>
</tr>
<tr>
<td>Industrial Competitors</td>
<td>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.</td>
</tr>
<tr>
<td>Disgruntled Employees</td>
<td>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.</td>
</tr>
<tr>
<td>Careless or Poorly Trained Employees</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Task 3. Specification of high level security requirements.**

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

There are many requirements documents that may be applicable to the Smart Grid. Currently, only NERC Critical Infrastructure Protection (CIP) standards are mandatory for the bulk electric system. The CSWG used three source documents for the cyber security requirements in this report—

- NERC CIP 002, 003-009, version 3;
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009; and

---

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

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 D, maps the Smart Grid security requirements in this report to the security requirements in SP 800-53, The DHS Catalog, and the NERC CIPs. Each requirement falls in one of three categories: governance, risk and compliance (GRC); common technical, and unique technical. The GRC requirements are applicable to all Smart Grid information systems within an organization and are typically implemented at the organization level and augmented, as required, for specific Smart Grid information systems. The common technical requirements are applicable to all Smart Grid information systems within an organization. The unique technical requirements are allocated to one or more of the logical interface categories defined in the logical reference model included in Chapter 4. Each organization must determine the logical interface categories that are included in each Smart Grid information system. These requirements are provided as guidance and are not mandatory. Each organization will need to perform a risk assessment to determine the applicability of the requirements to their specific situations.

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

Privacy Impact Assessment: Because the evolving Smart Grid presents potential privacy risks, a privacy impact assessment was performed. Several general privacy principles were used to assess the Smart Grid, and findings and recommendations were developed. The privacy recommendations provide a set of privacy requirements that should be considered when organizations implement Smart Grid information systems. These privacy requirements augment the security requirements specified in Chapter 5.


Using the conceptual model included in this report, the FERC 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 4 of this report. Because this is a high level logical reference model, there may be multiple implementations of the logical reference model. In the future, the Smart Grid conceptual reference model and the logical reference model will be used by the SGIP Architecture Committee (SGAC) in developing a single Smart Grid architecture. This overall Smart Grid
architecture will be used by the CSWG to revise the logical reference model included in this report.

**Task 4b. Assessment of Smart Grid standards.**

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

**Task 5. Conformity Assessment.**

The final task is to develop a conformity assessment program for security. This program will be SGIP.

### 1.4 Time Line

This final first version (v1.0) of NISTIR 7628 addresses the comments that were submitted in response to the first and second public drafts, which were posted for public review and comment. This version of NISTIR 7628 addresses all comments submitted to date, includes updated sections of the prior draft report, and includes a logical reference model, cryptography and key management issues, and guidance to assist individuals and organizations in using this report. Because the Smart Grid is evolving over time, the content of this report will need to be reviewed and updated as required.

### 1.5 Outstanding Issues and Remaining Tasks

The following areas need to be addressed in future versions of this report.

#### 1.5.1 Additional Cyber Security Strategy Areas

**Combined cyber-physical attacks:** The Smart Grid is vulnerable to coordinated cyber-physical attacks against its infrastructure. Assessing the impact of coordinated cyber-physical attacks will require a sound, risk-based approach because the Smart Grid will inherit all of the physical vulnerabilities of the current power grid (e.g., power outages caused by squirrels). Mitigating physical-only attacks is beyond the scope of this report, which is primarily focused on new risks and vulnerabilities associated with incorporating Smart Grid technologies into the existing power grid. The current version of this report is focused on assessing the impact of cyber-only vulnerabilities.

#### 1.5.2 Future Research and Development (R&D) Topics

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

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

1.5.3 Future Cryptography and Key Management Areas
Some topics that will be further developed in the future include:
• Smart grid adapted PKI: exploration of how to adapt PKI systems for the grid and its various operational and device/system requirements.
• Secure and trusted device profiles: development of a roadmap of different levels of hardware based security functionality that is appropriate for various types of Smart Grid devices.
• Applicable standards: identification and discussion of existing standards that can be used or adapted to meet the cryptography and key management requirements or solve the problems that have been identified.
• Certificate Lifetime: future work should be done to ensure that appropriate guidelines and best practices are established for the Smart Grid community.

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

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

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

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

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

- **Exploration of open and freely available standards:** Where appropriate, we will reference and discuss any open and freely available standards that can aid in addressing bottom-up problems, inform new and needed standards development, or help in design considerations.
CHAPTER TWO
HIGH LEVEL LOGICAL ARCHITECTURE

The NIST Framework and Roadmap document identifies seven domains within the Smart Grid: Transmission, Distribution, Operations, Bulk Generation, Markets, Customer, and Service Provider. A Smart Grid domain is a high-level grouping of organizations, buildings, individuals, systems, devices, or other actors with similar objectives and relying on—or participating in—similar types of applications. The various actors are needed to transmit, store, edit, and process the information needed within the Smart Grid.

The diagram below 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 in Chapter 4 of this report expand upon this high level diagram and include logical interfaces between actors and domains.
CHAPTER THREE
PRIVACY AND THE SMART GRID

CHAPTER ABSTRACT

The Smart Grid brings with it many new data collection, communication, and information sharing capabilities related to energy usage, and these technologies in turn introduce concerns about privacy. Privacy relates to individuals. Four dimensions of privacy are considered:

1. **Personal Information**—describes specific aspects of an individual;
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;
4. **Personal Communications Privacy**—the right to communicate without undue surveillance, monitoring, or censorship.

Most Smart Grid entities directly address the first dimension, because privacy of personal information is what most data protection laws and regulations cover. However, the other three dimensions are important privacy considerations as well and should be considered by Smart Grid entities.

When considering the possible legal impacts to privacy within the Smart Grid, and likewise the influence of laws that explicitly apply to the Smart Grid, it is important to note that current privacy laws do not explicitly reference the Smart Grid or associated unique Smart Grid data items. The innovative technologies of the Smart Grid pose new legal issues for privacy within the home and other properties.

The Smart Grid will greatly expand the amount of data that will be monitored, collected, aggregated, and analyzed. This expanded information, particularly from customer sites, raises added privacy concerns. For example, specific appliances and generators can be identified from the signatures they exhibit in electric information at the meter when collections occur with great frequency as opposed to through traditional monthly meter readings. This more detailed information expands the possibility of violating customer privacy.

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 these premises. The researchers’ conclusions based upon work in these primary areas are as follows:

- Evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, and premises create privacy risks and challenges that have not been tested and may or may not be mitigated by existing laws and regulations.
• New Smart Grid technologies, and particularly smart meters, smart appliances, and similar types of endpoints, create new privacy risks and concerns that may not be addressed adequately by the existing business policies and practices of utilities and third-party Smart Grid providers.

• Utilities and third-party Smart Grid providers need to follow standards to effectively and consistently safeguard the privacy of personal information.

• Consumers generally do not understand their privacy exposures or their options for mitigating those exposures within the Smart Grid.

Based on the research and the details of the associated findings, a summary listing of all recommendations includes the following points for entities that participate within the Smart Grid:

• Conduct a privacy impact assessment upon making the decision to deploy and/or participate in the Smart Grid. Such assessments should be updated following significant organizational, systems, applications, or legal changes—and particularly, following privacy breaches in addition to information security incidents involving personal information.

• 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 3.4.1 “Consumer-to-Utility PIA Basis and Methodology”). This should include appointing personnel responsible for ensuring privacy policies and protections are implemented.

• Provide regular privacy training and ongoing awareness communications and activities to all workers who have access to personal information within the Smart Grid.

• Develop privacy use cases that track data flows containing personal information to address and mitigate common privacy risks that exist for business processes within the Smart Grid.

• Educate consumers about the privacy risks within the Smart Grid and what they can do to mitigate them.

• Share information with other Smart Grid market participants concerning solutions to common privacy-related risks.

Additionally, manufacturers and vendors of smart meters, smart appliances, and other types of smart devices, should engineer these devices to collect only the data necessary for the purposes of the smart device operations. The defaults for the collected data should be established to use and share the data only as necessary to allow the device to function as advertised and used by Smart Grid consumers.
3.1 INTRODUCTION

Modernizing the current electric grid through the computerization and networking of intelligent components holds the promise of a Smart Grid infrastructure that can—

- Deliver electricity more efficiently;
- Provide better power quality;
- Link with a wide array of energy sources in addition to energy produced by power plants (such as renewable energy sources);
- Enable self-healing in cases of disturbance, physical and cyber attack, or natural disaster; and
- Provide consumers with more choices on how, when, and how much electricity they use.

Communications technology that enables the bi-directional flow of information throughout the infrastructure is at the core of these Smart Grid improvements, which rely upon collated energy usage data provided by smart meters, sensors, computer systems, and many other devices to 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 CSWG privacy subgroup 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 personal dwellings and electric vehicles. In July and August of 2009, the privacy subgroup performed a comprehensive privacy impact assessment (PIA) for the consumer-to-utility portion of the Smart Grid, and the results of this study have enabled the group to make the recommendations found in this chapter for managing the identified privacy risks.

The privacy subgroup membership is derived from a wide range of organizations and industries, including utilities, state utility commissions, privacy advocacy groups, academia, Smart Grid appliance and applications vendors, information technology (IT) engineers, and information security (IS) practitioners. This diversity of disciplines and areas of interest among the group’s participants helps ensure all viewpoints are considered when looking at privacy issues, and it brought a breadth of expertise both in recognizing inherent privacy risk areas and in identifying feasible ways in which those risks might be mitigated while at the same time supporting and maintaining the value and benefits of the Smart Grid.

Because this chapter will be read by individuals with a wide range of interests, professional fields, and levels of expertise with respect to Smart Grid privacy issues, careful consideration has been given to the chapter’s structure, which is as follows:

---

15 There may also be privacy concerns for individuals within business premises, such as hotels, hospitals, and office buildings, in addition to privacy concerns for transmitting Smart Grid data across country borders. However, because the existing collection of NIST use cases does not cover business locations or cross border data transmission, and in view of its time constraints, the Privacy Group did not research business premises or cross border privacy issues. The Privacy Group recommends these as topics for further investigation.
1. **Discussion of the concept of privacy.** This establishes our common ground in understanding the notion of “privacy” where readers may hold different viewpoints on the subject.

2. **Definitions of privacy terms.** Privacy terms are defined differently among various industries, groups, countries, and even individuals. We define the privacy terms used in this chapter.

3. **Overview of current data protection laws and regulations with respect to privacy.** Even though numerous laws exist to establish a range of privacy protections, it is important to consider how those privacy protections apply to the Smart Grid.

4. **Determination of personal activities within the Smart Grid.** This explains the creation of new data types in the Smart Grid, as well as new uses for data that has formerly only been in the possession of utilities outside of retail access states.\(^\text{16}\)

5. **Summary of the consumer-to-utility PIA.** Identifies key privacy issues identified by the privacy subgroup in performing its PIA for the consumer-to-utility portion of the Smart Grid and provides a guide for subsequent research.

6. **In-depth look at privacy issues and concerns.** Addresses follow-on research based on the PIA findings in which the privacy subgroup explored the broader privacy issues that exist within the entire expanse of the Smart Grid.

7. **Detailed analysis of representative privacy use cases.** Use cases can help Smart Grid architects and engineers build privacy protections into the Smart Grid. Some example privacy use cases were created for specific scenarios within the Smart Grid to identify privacy concerns and demonstrate how to use privacy use cases. Developers of Smart Grid applications, systems, and operational processes can employ a more comprehensive set of privacy use cases to create architectures that build in privacy protections to mitigate identified privacy risks.

8. **Conclusions and recommendations.** This section summarizes the main points and findings on the subject of privacy and collects in one place all the recommendations found within this Privacy Chapter.

9. **Appendices.** Reference material.

### 3.2 What Is Privacy?

Before describing the issues related to privacy within the Smart Grid, it is important to establish what we mean by that term. Because there is no one universal, internationally accepted definition of “privacy,” it can mean many things to different individuals. Privacy is not simply the specifications provided within laws and regulations. Privacy is not a plainly delineated concept. Furthermore, privacy should not be confused, as it often is, with being the same as confidentiality; and personal information is not the same as confidential information. Confidential information\(^\text{17}\) is information for which access should be limited to only those with a

\(^{16}\) “Retail access states” refers to those states offering programs whereby energy services companies may supply service to customers at market-based prices.

\(^{17}\) The use of the phrase “confidential information” in this document does not refer to National Security/classified information.
business need to know and that could result in compromise to a system, data, application, or other business function if inappropriately shared.\textsuperscript{18}

It is important to understand that privacy considerations with respect to the Smart Grid include examining the rights, values, and interests of \textit{individuals}; it involves the related characteristics, descriptive information and labels, activities, and opinions of individuals, to name just a few applicable considerations.

For example, some have described privacy as being comprised of four dimensions:\textsuperscript{19}

1. \textbf{Privacy of personal information}. This is the most commonly thought-of dimension. This information describes specific aspects about an individual. Privacy of personal information involves the right to control when, where, how, to whom, and to what extent an individual shares his or her 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. \textbf{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. \textbf{Privacy of personal behavior}. This is the right of individuals to make their own choices about what they do with respect to political activities, social activities, religious activities, etc. It also involves the right to keep the knowledge of certain personal behaviors from being shared with others.

4. \textbf{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, as the examples above themselves indicate, and also relate to some applicable laws and regulations; thus dimensions 2, 3, and 4 should also be considered to varying degrees in the Smart Grid setting.\textsuperscript{20}

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 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 within the Smart Grid are not new, there is now the possibility that many more individuals will have access to those data items; and there are now many new uses for the collected data, which may raise substantial privacy

\textsuperscript{18} For example, market data that does not include customer-specific details is considered confidential. Other chapters within this report address confidentiality in depth.

\textsuperscript{19} \textit{See}, Roger Clarke, "What’s Privacy?" at http://www.rogerclarke.com/DV/Privacy.html. Clarke makes a similar set of distinctions between the privacy of the physical person, the privacy of personal behavior, the privacy of personal 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.

\textsuperscript{20} For instance, consider the enhanced ability the Smart Grid will give to determining a person’s behavior within a home through more granular energy usage data.
impacts. As those data items become more specific and are made available to additional individuals, the complexity of the associated privacy impacts 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 existing Fair Information Principles\(^{21}\)
- 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.
- Making suggestions and providing information to organizations, regulatory agencies, and Smart Grid entities in the process of developing privacy policies and practices that promote and protect the interest of Smart Grid consumers and Smart Grid entities

To meet this mission, this chapter explores the types of data within the Smart Grid that may create privacy risks, in addition to exploring how existing types of data put into the Smart Grid could create privacy risks as a result of this new, always-connected type of technology network.

Because “privacy” and associated terms mean many different things to different audiences, definitions for the privacy terms used within this chapter are found in Appendix C and definitions for energy terms are included in Appendix I.

### 3.3 Legal Frameworks and Considerations

#### 3.3.1 Overview

In assessing privacy considerations and related legal impacts within the Smart Grid, it is important to understand existing regulatory and legislative frameworks, concepts, and definitions. This subsection discusses these themes in general terms and then narrows its focus to those deemed most relevant.

#### 3.3.2 Existing Regulatory Frameworks

When considering the possible legal impacts to privacy engendered by the Smart Grid, and likewise the influence of laws that directly apply to the Smart Grid, it is important to note that current privacy laws may not explicitly reference the Smart Grid or associated unique Smart Grid data items. Existing U.S. state-level Smart Grid and electricity delivery regulations may not explicitly reference privacy protections.\(^{22}\) However, even though they may not definitively reference the Smart Grid at this time, it is possible that existing laws may be amended to

---

\(^{21}\) Fair Information 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.

\(^{22}\) The SGIP-CSWG Privacy Group has compiled a list of most state Smart Grid and electricity delivery regulations and provided them within Appendix A as a useful resource for our readers.
explicitly apply to the Smart Grid as it is more widely implemented and touches more individuals.

While it is uncertain how privacy laws will apply to Smart Grid data, one thing that is certain is that the Smart Grid brings new challenges and issues with its new types of data, such as vehicle charging data. These new data items, and the use of existing data in new ways, will require additional study and public input to adapt current laws or to shape new laws.

To understand the types of data items that may be protected within the Smart Grid by privacy laws and regulations, let us first consider some of the current and most prominent laws that provide for privacy protection. U.S. federal privacy laws cover a wide range of industries and topics, such as:

1. Healthcare: Examples include the Health Insurance Portability and Accountability Act (HIPAA) and the associated Health Information Technology for Economic and Clinical Health (HITECH) Act.
2. Financial: Examples include the Gramm-Leach Bliley Act (GLBA), the Fair and Accurate Credit Transactions Act (FACTA), and the Red Flags Rule.
3. Education: Examples include the Family Educational Rights and Privacy Act (FERPA) and the Children’s Internet Protection Act (CIPA).
4. Communications: Examples include the First Amendment to the U.S. Constitution, the Electronic Communications Privacy Act (ECPA), and the Telephone Consumer Protection Act (TCPA).
6. Online Activities: Examples include the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act and the USA PATRIOT Act (commonly known as the "Patriot Act").
7. Privacy in the Home: Examples are the protections provided by the Fourth and Fourteenth Amendments to the U.S. Constitution.
8. Employee and Labor Laws: Examples include the Americans with Disabilities Act (ADA) and the Equal Employment Opportunity (EEO) Act.

It is currently unknown how or if the above laws providing privacy protections will be applied to Smart Grid data.

Each of the states provides additional privacy laws and regulations for a wide range of issues, such as for, but not limited to, the following, which may also apply to the Smart Grid:

- Privacy breach notice
- Social Security number (SSN) use and protections
- Drivers license use

---

23 The acronym stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. The statute enacted by the United States Government was signed into law on October 26, 2001.
There are generally three approaches to legally protecting privacy:

- **Constitutional protections.** The First, Fourth, and Fourteenth Amendments, covering personal communications and activities.
- **Data-specific protections.** These protect specific information items such as credit card numbers and SSNs, or specific technology such as phones or computers used for data storage or communication.
- **Contractual protections.** These are protections specifically outlined within a wide range of business contracts, such as those between customers and business.

It is possible that Fourth Amendment considerations would be applied to data collected about appliances and patterns of energy consumption, but this has not yet been tested. To the extent that Smart Grid data reveals information about personal activities, such as those described in “Privacy Concerns in the Smart Grid” (subsection 3.6 of this chapter) these may be considered to be Fourth Amendment issues in nature.

Even though public utilities commissions (PUCs) have protected energy data in some states such as California, the energy-related data produced by the Smart Grid may not be covered by privacy protection laws that name specific data items. Energy consumption patterns have historically not risen to the level of public concern given to financial or health data because (1) electrical meters had to be physically accessed to obtain usage data directly from buildings, (2) the data showed energy usage over a longer time span such as a month and did not show usage by specific appliance, and (3) the utilities were not sharing this data in the ways that will now be possible with the Smart Grid. Public concerns for the related privacy impacts will change with implementation of the Smart Grid, because energy consumption data can reveal personal activities and the use of specific energy using or generating appliances, and because the data may be used or shared in ways that will impact privacy.

While some states have examined the privacy implications of the Smart Grid, most states had little or no documentation available for review by the privacy subgroup. Furthermore, enforcement of state privacy-related laws is often delegated to agencies other than PUCs, who have regulatory responsibility for electric utilities.

### 3.3.3 Smart Grid Data Ownership

The legal ownership of Smart Grid energy data has been the subject of much discussion. Various regulators and jurisdictions have treated the issue of who owns energy data differently. However, regardless of data ownership, the management of energy data that contains or is combined with personal information or otherwise identifies individuals, and the personal information derived from such data, remains subject to the privacy considerations described in this report. The custodian of energy data should consider managing and safeguarding the information in accordance with the recommendations included in this report.

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

Personally identifiable information (PII) has no single authoritative legal definition. However, as noted in Appendix A, there are a number of laws and regulations, each of which protects different specific types of information. A number of these were previously noted, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which arguably has the
widest definition of PII within the existing U.S. federal regulations. State attorneys general have pointed to HIPAA as providing a standard for defining personal information, and to cite one case, the State of Texas has adopted the HIPAA requirements to be applicable to all types of organizations, including all those based out of Texas. Many of these organizations could possibly be providing information via the Smart Grid—if not now then almost certainly at sometime in the future.24

Private industry’s definition of PII predates legislation and is generally legally defined in a two-step manner, as \( x \) data (e.g., SSN) in conjunction with \( y \) data (e.g., name.) This is the legal concept of “personally identifiable information” or PII.

For example, the Massachusetts data breach law,25 in line with some other state breach notice laws, defines the following data items as being PII:

First name and last name or first initial and last name in combination with any one or more of the following:
1. Social Security number;
2. Driver's license number or state-issued identification card number; or
3. Financial account number.

Utilities often store SSNs and financial account numbers in their payroll or billing systems and have been obligated to follow the associated legal requirements for safeguarding this data for many years. The sharing and storage capabilities that the Smart Grid network brings to bear creates the new need to protect the items specifically named within existing laws, in addition to protecting new types of personal information that is created within the Smart Grid. There is also the possibility of utilities possessing new types of data as a result of the Smart Grid for which they have not to date been custodians. These new types of data may be protected by regulations from other industries that utilities did not previously have to follow. As is revealed by the privacy impact assessment that is the subject of subsection 3.4 of this chapter, there is a lack of privacy laws or policies directly applicable to the Smart Grid. Privacy subgroup research indicates that, in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid.26 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.27

---

24 For example, the Texas Appellate Court clearly said that the HIPAA Privacy rule applies to the entire State of Texas. See, Abbott v. Texas Department of Mental Health and Mental Retardation for details, or refer to the discussion at http://www.hipaasolutions.org/white_papers/HIPAA%20Solutions,%20LC%20White%20Paper%20Texas%20AG%20Opinion%20On%20Privacy%20And%20HIPAA.pdf.


26 Most public utility commissions do have significant customer privacy policies that predate the Smart Grid, which the Privacy Group determines most utilities contacted take very seriously.

27 Edison Electric Institute, the trade association of investor-owned electric utilities, is developing a formal position on customer data access, which it expects to finalize during 2010.
The privacy subgroup is presently conducting an overview of the laws, regulations, and standards relevant to the privacy of energy consumption data, and its preliminary list of applicable state laws and regulations is given in Appendix A.

### 3.3.5 General Invasion of Privacy Concerns with Smart Grid Data

Two aspects of the Smart Grid may raise new legal privacy issues. First, the Smart Grid significantly expands the amount of data available in more granular form as related to the nature and frequency of energy consumption and creation, thereby opening up more opportunities for general invasion of privacy. Suddenly a much more detailed picture can be obtained about activities within a given dwelling, building, or other property, and the time patterns associated with those activities make it possible to detect the presence of specific types of energy consumption or generation equipment. Granular energy data may even indicate the number of individuals in a dwelling unit, which could also reveal when the dwelling is empty or is occupied by more people than usual. The public sharing of information about a specific location’s energy use is also a distinct possibility. For example, a homeowner rigged his washing machine to announce the completion of its cycle via his social networking page so that the machine need not be monitored directly.  

This raises the concern that persons other than those living within the dwelling but having access to energy data could likewise automate public sharing of private events without the dwellers’ consent—a general invasion of privacy.

The concern exists that the prevalence of granular energy data could lead to actions on the part of law enforcement—possibly unlawful in themselves—and lead to an invasion of privacy that could be potentially harmful to the dwelling’s residents. Law enforcement agencies have already used monthly electricity consumption data in criminal investigations. For example, in *Kyllo v. United States*, the government relied on monthly electrical utility records to develop its case against a suspected marijuana grower. Government agents issued a subpoena to the suspect’s utility to obtain energy usage records and then used a utility-prepared “guide for estimating appropriate power usage relative to square footage, type of heating and accessories, and the number of people who occupy the residence” to show that the suspect’s power usage was “excessive” and thus “consistent with” a marijuana-growing operation.

As Smart Grid technologies collect more detailed data about households, the concern is that law enforcement officials may become more interested in accessing that data for investigations or to develop cases. For instance, agencies may want to establish or confirm presence at an address at a certain critical time or even establish certain activities within the home—information that may be readily gleaned from Smart Grid data.

---

28 For a demonstration of how this was done, see the video, "Washing Machine Twitter Hack," by Ryan Rose at [http://vimeo.com/2945872](http://vimeo.com/2945872).


30 *Id.* at 30. The Supreme Court opinion in this case focuses on government agents’ use of thermal imaging technology. However, the district court decision discusses other facts in the case, including that government agents issued a subpoena to the utility for the suspect’s monthly power usage records. *See United States v. Kyllo*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff’d*, 190 F.3d 1041 (9th Cir. 1999), *rev’d*, 533 U.S. 27 (2001).

However, the Supreme Court in *Kyllo* clearly reaffirmed the heightened Fourth Amendment privacy interest in the home and noted this interest is not outweighed by technology that allows government agents to “see” into the suspect’s home without actually entering the premises.32 The Court stated, “We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search” and is “presumptively unreasonable without a warrant.”33

Second, unlike the traditional energy grid, the Smart Grid may be viewed as carrying private electronic communications between utilities and end-users, 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.34 Moreover, under the Communications Assistance for Law Enforcement Act (CALEA), telecommunications carriers and equipment manufacturers are required to design their systems to enable lawful access to communications.35 The granular Smart Grid data may also have parallels to call detail records collected by telecommunications providers. It is unclear if laws that regulate government access to communications will also apply to the Smart Grid.

In short, the innovative technologies of the Smart Grid pose new legal issues for privacy of the home, as well as any type of property location that has traditionally received strong Fourth Amendment protection. As Justice Scalia wrote in *Kyllo*: “The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.”36

### 3.3.6 Smart Grid Introduces a New Privacy Dimension

The ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical to the major benefits of the Smart Grid—and it is also a significant concern from a privacy viewpoint, especially when this data and data extrapolations are associated with individual consumers or locations. Some articles in the public media have raised serious concerns37 about the type and amount of billing, usage, appliance, and other related information flowing throughout the various components of the Smart Grid.

Figure 3-1 illustrates how frequent meter readings may provide not only a detailed timeline of activities occurring inside a metered location but could also lead to knowledge about specific equipment usage or other internal home/business processes.

---

32 *Kyllo*, 533 U.S. 27.

33 *Kyllo*, 533 U.S. at 34, 40.

34 Such as the Electronic Communications Privacy Act; 18 U.S.C. § 2510. See [http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_1_20_119.html](http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_1_20_119.html).


Smart meter data raises potential surveillance possibilities posing physical, financial, and reputational risks. Because smart meters collect energy usage data at much shorter time intervals than in the past (in 15-minute or sub-15-minute intervals rather than once a month), the information they collect can reveal much more detailed information about the activities within a dwelling or other premises than was available in the past. This is because smart meter data provides information about the usage patterns for individual appliances—which in turn can reveal detailed information about activities within a premise through the use of nonintrusive appliance load monitoring (NALM) techniques. Using NALM, appliances’ energy usage profiles can be compared to libraries of known patterns and matched to identify individual appliances. For example, research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home

---


39 *Id.* at A-2. The development of NALM involved a real-time monitoring device attached to a meter to log energy consumption. Researchers then worked backward from that information using complex algorithms to reconstruct the presence of appliances. Since smart meters and these NALM devices operate similarly, the same research and techniques can be reused to identify appliances.

40 *Id.* at A-4 n.129 (discussing the maintaining of appliance profile libraries).
appliances. The graph shown above (Figure 3-1) depicts NALM results as applied to a household’s energy use over a 24-hour period. NALM techniques have many beneficial uses, including pinpointing loads for purposes of load balancing or increasing energy efficiency. However, such detailed information about appliance use can also reveal whether a building is occupied or vacant, show residency patterns over time, and reflect intimate details of people’s lives and their habits and preferences inside their homes. In 1989, George W. Hart, one of the inventors of NALM, explained the surveillance potential of the technique in an article in IEEE Technology and Society Magazine. As the time intervals between smart meter data collection points decreases, appliance use will be inferable from overall utility usage data and other Smart Grid data with even greater accuracy.

In general, more data, and more detailed data, may be collected, generated, and aggregated through Smart Grid operations than previously collected through monthly meter readings and distribution grid operations. Figure 3-2 presents the NIST conceptual model illustrating how data collection can be expected to proliferate as networked grid components increase. In addition to utilities, new entities may also seek to collect, access, and use smart meter data (e.g., vendors creating applications and services specifically for smart appliances, smart meters, and other building-based solutions). Further, once uniquely identifiable “smart” appliances are in use, they will communicate even more specific information directly to utilities, consumers, and other entities, thus adding to the detailed picture of activity within a premise that NALM can provide.


43 For instance, daily routines such as showers and baths could be identified, as well as whether the customer “prefers microwave dinners to a three-pot meal.” Id. Quinn, Privacy and the New Energy Infrastructure, at 5.

The proliferation of smart appliances, utility devices, and devices from other entities throughout the Smart Grid, on both sides of the meter, means an increase in the number of devices that may generate data. The privacy risks presented by these smart appliances and devices on the customer side of the meter are expanded when these appliances and devices transmit data outside of the home area network (HAN) or energy management system (EMS) and do not have documented security requirements, effectively extending the perimeter of the system beyond the walls of the premises.

Data may also be collected from plug-in electric vehicles (PEVs). Charging data may be used to track the travel times and locations for the PEV owners.

### 3.4 Consumer-to-Utility Privacy Impact Assessment

A PIA is a comprehensive process for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information. PIAs also define the measures that may be used to mitigate and, wherever possible, eliminate the identified risks. The Smart Grid PIA activity provides a structured, repeatable, type of analysis aimed at determining how collected data can reveal personal information about individuals or groups of individuals, and the focus of the PIA can be on a segment within the grid or the grid as a whole. Privacy risks

---

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 additionally considered the privacy impacts and risks throughout the entire Smart Grid structure.

The focus of the privacy subgroup has been on determining (1) the types of information that may be collected or created that can then reveal information about individuals or activities within specific premises (both residential and commercial), (2) determining how these different types of information may be exploited, and (3) recommending business policies and practices to mitigate the identified privacy risks. Entities of all types that provide, use, or obtain data from the Smart Grid can also benefit from performing PIAs to determine privacy risks and then take action to mitigate those risks.

The following questions were identified and addressed in the process of performing the consumer-to-utility PIA and in the follow-on discussion of the findings:

1. What personal information may be generated, stored, transmitted, or maintained by components of the Smart Grid?
2. How is this personal information new or unique compared with personal information in other types of systems and networks?
3. How is the use of personal information within the Smart Grid new or different from the uses of the information in other types of systems and networks?
4. What are the new and unique types of privacy risks that may be created by Smart Grid components and entities?
5. What is the potential that existing laws, regulations, and standards apply to the personal information collected by, created within, and flowing through the Smart Grid components?
6. What could suggested privacy principles look like for all entities using the Smart Grid so that following them could help to protect privacy and reduce associated risks?

### 3.4.1 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)\(^{46}\) and other published Smart Grid plans covering the interactions between the consumers of services and the providers of those services. The group also reviewed numerous data protection requirements and considered global information security and privacy protection laws, regulations, and standards to assemble the criteria against which to evaluate the consumer-to-utility aspects of Smart Grid operations. Taken into account were numerous U.S. federal data protection requirements and Fair Information Principles, also often called “Privacy Principles,” that are the framework for most modern privacy laws around the world. Several versions of the

---

Fair Information Principles have been developed through government studies, federal agencies, and international organizations.

For the purposes of this PIA the group specifically used the American Institute of Certified Public Accounts (AICPA) Generally Accepted Privacy Principles (GAPP), the Organisation for Economic Cooperation and Development (OECD) Privacy Principles, and principles from the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) International Standard ISO/IEC 27001 as its primary evaluation criteria:

- The ten AICPA principles are entitled Management, Notice, Choice and Consent, Collection, Use and Retention, Access, Disclosure to Third Parties, Security for Privacy, Quality, and Monitoring and Enforcement.

- With respect to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 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, wherein paragraphs 7–14 of Part Two outline the basic principles of national application, and on the “Explanatory Memorandum,” wherein those principles are amplified (by paragraph number) in subsection II.B. The enumerated OECD principles relate to Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Openness, and Individual Participation.


The general privacy principles 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 requirements. However, most data protection laws throughout the world have been built around these principles.

### 3.4.2 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

---


49 See, full OECD “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” at http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html.

50 Id. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#guidelines.

51 Id. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2.

52 Id. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#memorandum.

53 Id. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#comments.
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 subsection 3.3.54 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 subgroup’s PIA findings to develop appropriate systems and processes for the Smart Grid data. Organizations can also conduct their own PIAs using the six questions listed in subsection 3.4 and then communicate the findings listed with the ten privacy principles listed below. The answers to these questions are essential both for efficient data management in general and for developing an approach that will address privacy impacts.

Where an organization has defined privacy responsibilities, policies, and procedures, that organization should consider reviewing its responsibilities and updating or potentially augmenting its policies and procedures to address the new privacy issues associated with the Smart Grid. Each entity within the Smart Grid can follow a similar methodology to perform its own PIAs to ensure privacy is appropriately addressed for its Smart Grid activities.

The following points summarize the PIA findings and recommendations as presented in the draft NIST Smart Grid High Level Consumer-to-Utility Privacy Impact Assessment55 in relation to the privacy principles used as the basis for the PIA. Each enumerated privacy principle statement is followed by the related findings from the PIA and the suggested privacy practices that may serve to mitigate the privacy risks associated with each principle:

1. **Management and Accountability**: Organizations that access or provide data to the Smart Grid should appoint personnel to a position responsible for ensuring that documented information security and privacy policies and practices exist and are followed. IS and PII 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.

---

54 See, 3.3.2, “Existing Regulatory Frameworks,” and 3.3.4, “Applicability of Existing Data Protection Laws and Regulations to the Smart Grid.”

Privacy Practices Recommendations:

- **Assign privacy responsibility.** Each organization collecting or using Smart Grid data from or about consumer locations should create (or augment) a position or person with responsibility to ensure privacy policies and practices exist and are followed. Responsibilities should include documenting, ensuring the implementation of, and managing requirements for regular training and ongoing awareness activities.

- **Establish privacy audits.** Audit functions should be modified to monitor all energy data access.

- **Establish law enforcement request policies and procedures.** Organizations accessing, storing, or processing energy data should include specific documented incident response procedures for incidents involving energy data.

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

**Findings:**

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

Privacy Practices Recommendations:

- **Provide notification for the personal information collected.** Any organization collecting energy data from or about consumers should establish a process to notify consumer account inhabitants and person(s) paying the bills (which may be different entities), when appropriate, of the data being collected, why it is necessary to collect the data, and the intended use, retention, and sharing of the data. This notification should include information about when and how information may or may not be shared with law enforcement officials. Data subjects should be notified before the time of collection.

- **Provide notification for new information use purposes and collection.** Organizations should update customer notifications whenever they want to start using existing collected data for materially different purposes other than those the consumer has previously authorized. Also, organizations should notify the recipients of services whenever they want to start collecting additional data beyond that already being collected, along with providing a clear explanation for why the additional data is necessary.

3. **Choice and Consent:** The organization should describe the choices available to consumers with regard to the use of their associated energy data that could be used to reveal personal information and obtain explicit consent, if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of this information.
Findings:
Currently it is not apparent that utilities or other entities within the Smart Grid obtain consent to use the personal information generated and collected for purposes other than billing. As smart meters and other smart devices increase capabilities and expand sharing of the data throughout the Smart Grid, organizations should establish processes to give consumers a choice, where possible and feasible, about the types of data collected and how it is used.

Privacy Practices Recommendations:

- **Provide notification about choices.** The consumer notification should include a clearly worded description to the recipients of services notifying them of (1) any choices available to them about information being collected and obtaining explicit consent when possible; and (2) explaining when and why data items are or may be collected and used without obtaining consent, such as when certain pieces of information are needed to restore service in a timely fashion.

4. **Collection and Scope:** Only personal information that is required to fulfill the stated purpose should be collected from consumers. This information should be obtained by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.

Findings:
In the current operation of the electric utilities, data taken from traditional meters consists of basic data usage readings required to create bills. Under the Smart Grid implementation, smart meters will be able to collect other types of data. Home power generation services will also likely increase the amount of information created and shared. Some of this additional data may constitute personal information or may be used to determine personal activities. Because of the associated privacy risks, only the minimum amount of data necessary for services, provisioning, and billing should be collected.

Privacy Practices Recommendations:

- **Limit the collection** of data to only that necessary for Smart Grid operations, including planning and management, improving energy use and efficiency, account management, and billing.
- **Obtain the data** by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.

5. **Use and Retention:** Information within the Smart Grid should only be used or disclosed for the purposes for which it was collected and should only be shared, in any form, with those parties authorized to receive it. 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 only be kept as long as is necessary to fulfill the purposes for which it was collected.
Findings:
In the current operation of the electric utilities, data taken from traditional meters is used to create consumer bills, determine energy use trends, and allow consumers to control their energy usage both on-site and remotely. The Smart Grid will provide data that can be used in additional ways not currently possible.

Privacy Practices Recommendations:

- **Review privacy policies and procedures.** Every organization with access to Smart Grid data should review existing information security and privacy policies to determine how they may need to be modified. This review should include privacy policies already in place in other industries, such as financial and healthcare, which could provide a model for the Smart Grid.

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

6. **Individual Access:** Organizations should provide a process to allow for data subjects to request access to see their corresponding personal information and energy data, and to request the correction of perceived inaccuracies. Personal information data subjects 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:

- **Customer 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 and energy data should be used only for the purposes for which it was collected. Personal information should not be disclosed to any other parties except those identified in the notice or with the explicit consent of the service recipient.
Findings:
As Smart Grid implementations collect more granular and detailed information, this information is potentially revelatory of activities and equipment usage in a given location. As this information may reveal business activities, manufacturing procedures, and personal activities, significant privacy concerns and risks arise when the information is disclosed without the knowledge, consent, and authority of the individuals or organizations to which the information applies.

Privacy Practices Recommendations:

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

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

Findings:
Smart Grid data may be transmitted to and stored in multiple locations throughout the Smart Grid. Establishing strong security safeguards is necessary to protect energy data from loss, theft, unauthorized access, disclosure, copying, use, or modification.

Privacy Practices Recommendations:

- **Associate energy data with individuals only when and where required.** For example only link equipment data with a location or consumer account when needed for billing, service restoration, or other operational needs. This practice is already common in the utility industry and should be maintained and applied to all entities obtaining or using this data as the Smart Grid is further deployed.

- **De-identify information.** Energy data and any resulting information, such as monthly charges for service, collected as a result of Smart Grid operations should be aggregated and anonymized by removing personal information elements wherever possible to ensure energy data from specific consumer locations is limited appropriately. This may not be possible for some business activities, such as for billing.

- **Safeguard personal information.** All organizations collecting, processing, or handling energy data and other personal information from or about consumer locations should ensure that all information collected and subsequently created about the recipients of Smart Grid services is appropriately protected in all forms from loss, theft, unauthorized access, disclosure, copying, use, or modification. While this practice is commonly in effect in the utility industry, as other entities recognize commercial uses for this information, they too should adopt appropriate requirements and controls. In addition, given the growing granularity of information from Smart
Grid operations, the responsibility for these existing policies should be reviewed and updated as necessary.

- **Don’t 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 sufficiently anonymized and/or aggregated to assure to a reasonable degree the inability to link detailed data to individuals. Current and planned research is being conducted both inside and outside the utility industry on the Smart Grid, its effects upon demand response, and other topics. The use of actual information that can be linked to a consumer in this research increases the risk of inadvertent exposure via traditional information sharing that occurs within the research community.

9. **Accuracy and Quality:** Processes should be implemented by all businesses participating within the Smart Grid to ensure as much as possible that energy data and personal information are accurate, complete, and relevant for the purposes identified in the notice [See §3.4.2-2], and that it remains accurate throughout the life of the energy data and personal information while within the control of the organization.

**Findings:**
The data collected from smart meters and related equipment will potentially be stored in multiple locations throughout the Smart Grid. Smart Grid data may be automatically collected in a variety of ways. Establishing strong security safeguards will be necessary to protect the information and the information’s accuracy. Since Smart Grid data may be stored in many locations, and therefore be accessed by many different individuals/entities and used for a wide variety of purposes, personal information may be inappropriately modified. Automated decisions about energy use could be detrimental for consumers (e.g., restricted power, thermostats turned to dangerous levels, and so on) if it happens that decisions about energy usage are based upon inaccurate information.

**Privacy Practices Recommendations:**

- **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 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.

**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.

Privacy Practices Recommendations:

- **Policy challenge procedures.** Organizations collecting energy data, and all other entities throughout the Smart Grid, should establish procedures that allow Smart Grid consumers to have the opportunity and process to challenge the organization’s compliance with their published privacy policies as well as their actual privacy practices. This becomes more important as energy data becomes more granular, more refined, and has more potential for commercial uses.

- **Perform regular privacy impact assessments.** Any organization collecting energy data from or about consumer locations should perform periodic PIAs with the proper timeframes, to be determined by the utility and the appropriate regulator, based upon the associated risks and any recent process changes and/or security incidents. The organizations should consider sending a copy of the PIA results to the appropriate state privacy office for review. This will help to ensure compliance with appropriate state policies 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 to the appropriate state privacy office for review.

- **Establish breach notice practices.** Any organization with Smart Grid data should establish policies and procedures to identify breaches and misuse of Smart Grid data, along with expanding or establishing procedures and plans for notifying the affected individuals in a timely manner with appropriate details about the breach. This becomes particularly important with new possible transmissions of billing information between utilities and other information between utilities and other entities providing services in a Smart Grid environment (e.g., third party service providers).

### 3.5 PERSONAL INFORMATION IN THE SMART GRID

As the PIA detailed, energy data and personal information can reveal something either explicitly or implicitly about specific individuals, groups of individuals, or activities of those individuals. Smart Grid data such as energy usage measurements, combined with the increased frequency of usage reporting, energy generation data, and the use of appliances and devices capable of energy consumption reporting, provide new sources of personal information.

The personal information traditionally collected by utility companies can be used to identify individuals through such data as house number and/or street address, homeowner or resident’s first, middle, or last name, date of birth, and last four digits of the SSN. Smart Grid data elements that reflect the timing and amount of energy used, when correlated with traditional personal information data elements, can provide insights into the life style of residential customers and the business operations of commercial and industrial customers.\(^{56}\)

---

\(^{56}\) The ability to determine personal activities according to energy consumption data alone was demonstrated recently in quotes from a Siemens representative in an article published in the Washington Post: "We, Siemens, have
With a few exceptions (e.g., SSN and credit card numbers), rarely does a single piece of information or a single source permit the identification of an individual or group of individuals. However, in recent years it has been shown through multiple research studies and incidents that a piece of seemingly anonymous data (date of birth, gender, zip code) that on its own cannot uniquely identify an individual may reveal an individual when combined with other types of anonymous data. If different datasets that contain anonymized data have at least one type of information that is the same, the separate sets of anonymized information may have records that are easily matched and then linked to an individual. It is also possible the matches to an individual may be narrowed to the point that linking becomes an easy task. (This may particularly be seen in sparsely populated geographical areas.)

There are potential unintended consequences of seemingly anonymous Smart Grid data being compiled, stored, and cross-linked. One concern is that combining Smart Grid data, which may be considered anonymous, with other types of anonymous information might lead to identifying individuals or groups of individuals associated with an address. Computing technology and the use of certain algorithms makes this type of process much easier.

While current privacy and security anonymization practices tend to focus on the removal of specific PII data items, the studies referenced in this subsection show that re-identification and

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,” Washington Post, June 25, 2010; http://www.washingtonpost.com/wp-dyn/content/article/2010/06/25/AR2010062501686.html.

57 See, Arvind Narayanan and Vitaly Shmatikov, Privacy and Security: Myths and Fallacies of “Personally Identifiable Information”, Communications of the ACM, at http://userweb.cs.utexas.edu/~shmat/shmat_cacm10.pdf. June, 2010. This article points out multiple incidents and studies that have shown how combinations of data items that are anonymous individually can be linked to specific individuals when combined with other anonymous data items and “quasi-identifiers” or a piece of auxiliary information. “Consumption preferences” is specifically named as a type of human characteristic data that, when combined with other items, can point to individuals.

58 In addition to the incidents discussed in the Narayanan and Shmatikov article previously referenced, another specific example to consider is that in 2006 AOL released anonymous information about search data that was re-identified linking to individuals by a NY Times reporter. This incident led to a complaint filed by the Electronic Frontier Foundation (EFF) with the Federal Trade Commission against AOL for violating the Federal Trade Commission Act. See, Michael Barbaro & Tom Zeller, Jr., A Face is Exposed for AOL Searcher No. 4417749, N.Y. TIMES, Aug. 9, 2006, at A1, available at http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000.

59 Latanya Sweeney, k-anonymity: A Model for Protecting Privacy, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(5), 2002; 557-570, available at http://epic.org/privacy/reidentification/Sweeney_Article.pdf. Sweeney gathered data from the Massachusetts Group Insurance Commission (GIC), which purchases health insurance for state employees. GIC released insurer records to the researcher, but before doing so, with the support of the Governor’s office, they removed names, addresses, SSNs, and other “identifying information” in order to protect the privacy of the employees. Sweeney then purchased voter rolls, which included the name, zip code, address, sex, and birth date of voters in Cambridge. Matched with the voter rolls, the GIC database showed only six people in Cambridge were born on the same day as the governor, half of them were men, and the governor was the only one who lived in the zip code provided by the voter rolls. Correlating information in the voter rolls with the GIC database made it possible to re-identify the governor’s records in the GIC data, including his prescriptions and diagnoses.
linking to an individual may still occur. This issue of data re-identification potentially becomes 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 activities.

Table 3-1 identifies and describes potential data elements within the Smart Grid that could impact privacy if not properly safeguarded.

### Table 3-1 Information potentially available through the Smart Grid

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

### 3.6 IN-DEPTH LOOK AT SMART GRID PRIVACY CONCERNS

As outlined within 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 customer acceptance and participation, if not outright litigation.

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

- **Type I**: Personal information not previously readily obtainable.
- **Type II**: Mechanisms for obtaining (or manipulating) personal information that did not previously exist.
Examples of Type I concerns include detailed information on the appliances and equipment in use at a given location and finely grained time series data on power consumption at metered locations and from individual appliances.

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

Detailed pictures of activities within a house or building can be derived from “equipment electricity signatures” and their time patterns. Such signatures and patterns can provide a basis for making assumptions about occupant activities (e.g., the number of individuals at a location and when the premise was unoccupied).

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

Table 3-2 outlines some of the possible areas of privacy concern and provides some analysis of the nature of the concern according to the Type I and II categories given above. While this is not an exhaustive list, it serves to help categorize the concerns noted.

<table>
<thead>
<tr>
<th>Privacy Concern</th>
<th>Discussion</th>
<th>Categorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td>Attributing energy consumption to another location or vehicle (in the case of PEVs).</td>
<td>Type II: While fraud is an existing concern, the current system of reading customer meters (either manual recording or electronically via “drive-by” remote meter reading systems) may allow less opportunity for data manipulation without collusion with the personnel collecting the data.</td>
</tr>
<tr>
<td>Determine Personal Behavior Patterns / Appliances Used</td>
<td>Smart meter and home automation network data may track the use of specific appliances. Access to data-use profiles that can reveal specific times and locations of electricity use in specific areas of the home can also indicate the types of activities and/or appliances used. Appliance manufacturers may want to get this information to know who, how, and why individuals used their products. Such information could impact appliance warranties.</td>
<td>Type I: The type of data made available by Smart Grid implementation may be both more granular and available on a broader scale.</td>
</tr>
</tbody>
</table>

---

60 This is a term coined by our Privacy Group and not one that is officially used by any regulatory or standards group.
### Privacy Concern Discussion Categorization

<table>
<thead>
<tr>
<th>Privacy Concern</th>
<th>Discussion</th>
<th>Categorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform Real-Time Remote Surveillance</td>
<td>Access to live energy use data can reveal such things as if people are in a facility or residence, what they are doing, waking and sleeping patterns, where they are in the structure, and how many are in the structure.</td>
<td>Type II: Many methods of real-time surveillance currently exist. The availability of computerized real-time or near-real-time energy usage data would create another way in which such surveillance could be conducted.</td>
</tr>
<tr>
<td>Non-Grid Commercial Uses of Data</td>
<td>Personal energy consumption data storage may reveal lifestyle information that could be of value to many entities, including vendors of a wide range of products and services. Vendors may purchase attribute lists for targeted sales and marketing campaigns that may not be welcomed by those targets. Universities might purchase information to study student attributes and target a new student profile with simple application question profiling. Such profiling could extend to other types of profiling on employment selection, rental applications, and other situations that may not be welcomed by those targets.</td>
<td>Type II: Under the existing metering and billing systems, meter data is not sufficiently granular in most cases to reveal any detail about activities. However, smart meters, time of use and demand rates, and direct load control of equipment may create detailed data that could be sold and used for energy management analyses and peer comparisons. While this information has beneficial value to third parties, consumer education about protecting that data has considerable positive outcomes.</td>
</tr>
</tbody>
</table>

#### 3.6.1 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 the like, as illustrated at the beginning of this chapter (subsection 3.3.6, Figure 3-1). Especially when considered over a period of time, this information can provide a basis for making assumptions about occupant activities and lifestyle. For example, assumptions may be made about the number of individuals at a premise, when the location is unoccupied, sleep schedules, work schedules, and other personal routines.  

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

---

61 See, Mikhail Lisovich, Deirdre Mulligan, & Stephen Wicker, *Inferring Personal Information from Demand-Response Systems*, IEEE Security & Privacy, Jan.-Feb. 2010, at 11-20 (presenting the results of an initial study in the types of information than can be inferred from granular energy consumption data).
example, residential demand-response systems,\textsuperscript{62} marketing,\textsuperscript{63} and law enforcement.\textsuperscript{64} 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 3-2), outlines some of the likely uses of Smart Grid data and maps them to privacy concerns that arise from new uses. The table also lists a variety of parties that are likely to use Smart Grid data. Many of these uses are legitimate and beneficial. However, all parties that collect and use Smart Grid data should be aware of uses that impact privacy and should develop appropriate plans for data stewardship, security, and data use. Any party could intentionally or unintentionally be the source of data that is misused or that is used in a way that has negative effects on customer privacy. “Intentional” privacy compromises might occur through voluntary disclosure of data to third parties who then share the data with others or use the data in unexpected ways, while “unintentional” impacts might arise through data breaches or criminal attacks. It is important that all Smart Grid entities handling personal information to be aware of the various possible uses of the data and that they consider these factors when developing processes for data collection, handling, and disclosure.

Many potential uses arise from the generation of granular energy data, especially when it is combined with PII. Table 3-3 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.


\textsuperscript{63} Martin LaMonica, Microsoft Dials Hohm to Cut Home Energy Use, CNET, June 23, 2009, available at http://news.cnet.com/8301-11128_3-10269832-54.html (describing Microsoft’s business model for monetizing its energy consumption web application as selling contextual ads to generate revenue in the beginning, but eventually “Microsoft anticipates that it can become a sort of information broker between customers and utilities looking for ways to improve the efficiency of their customers”).

\textsuperscript{64} Law enforcement already uses energy consumption data to try to identify potentially criminal activity, like drug cultivation. See, e.g., Jo Moreland, Drug Raid Has Carlsbad Family Seeing Red, N. County Times, Mar. 25, 2004, available at http://www.nctimes.com/news/local/article_ea2047e8-59e1-551e-b173-ce89ffad4d90.html. More granular data will provide them with more valuable information that may be able to identify a wider range of illegal activities.
Table 3-3 Potential Privacy Impacts that Arise from the Collection and Use of Smart Grid Data

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Privacy-Related Information Potentially Revealed by this Type of Data</th>
<th>Parties Potentially Collecting or Using this Type of Data</th>
<th>Type of Potential Use</th>
<th>Specific Potential Uses of this Type of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captures detailed energy usage at a location, whether in real-time or on a delayed basis.</td>
<td><strong>Personal Behavior Patterns and Activities Inside the Home</strong> 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. <strong>Real-Time Surveillance Information</strong> Via real-time energy use data, determine if anyone is home, what they are doing, and where they are located in the home.</td>
<td>Utilities</td>
<td>Primary</td>
<td>Load monitoring and forecasting; demand response; efficiency analysis and monitoring, billing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edge Services</td>
<td>Secondary</td>
<td>Efficiency analysis and monitoring; demand-response, public or limited disclosure to promote conservation, energy awareness, etc. (e.g., posting energy usage to social media).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Insurance Companies</td>
<td></td>
<td>Determine premiums (e.g. specific behavior patterns, like erratic sleep, that could indicate health problems).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketers</td>
<td></td>
<td>Profile for targeted advertisements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Law Enforcement</td>
<td></td>
<td>Identify suspicious or illegal activity; investigations; real-time surveillance to determine if residents are present and current activities inside the home.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Civil Litigation</td>
<td></td>
<td>Determine when someone was home or the number of people present.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Landlord/Lessor</td>
<td></td>
<td>Use tenants’ energy profiles to verify lease compliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Private Investigators</td>
<td></td>
<td>Investigations; monitoring for specific events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Press</td>
<td></td>
<td>Public interest in the activities of famous individuals.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creditors</td>
<td></td>
<td>Determine behavior that seems to indicate creditworthiness or changes in credit risk.</td>
</tr>
</tbody>
</table>

65 “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.

66 Edge services include businesses providing services based directly upon electrical usage but not providing services related to the actual generation, transportation, or distribution of electricity. Some examples of edge services would include Google PowerMeter, Microsoft Hohm, or consulting services based upon electricity usage.

67 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, Feb. 28, 2007, available at http://www.foxnews.com/story/0,2933,254908,00.html.

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Privacy-Related Information Potentially Revealed by this Type of Data</th>
<th>Parties Potentially Collecting or Using this Type of Data</th>
<th>Type of Potential Use</th>
<th>Specific Potential Uses of this Type of Data</th>
</tr>
</thead>
</table>
| Identifies location / recharge information for PEVs or other location-aware appliances. | *Determine Location Information*  
Historical PEV data, which can be used to determine range of use since last recharge.  
Location of active PEV charging activities, which can be used to determine the location of driver. | Utilities                                                                 | Primary               | Bill energy consumption to owner of the PEV; distributed energy resource management; emergency response.                                                                                                                                                               |
|                                                                             |                                                                                                                                   | Insurance Companies | Secondary             | Determine premiums based on driving habits and recharge location.                                                                                                                                                                                                 |
|                                                                             |                                                                                                                                   | Marketers                                                        |                      | Profile and market based on driving habits and PEV condition.                                                                                                                                                                                                  |
|                                                                             |                                                                                                                                   | Law Enforcement/ Agencies                                       |                      | Investigations; locating or creating tracking histories for persons of interest.                                                                                                                                                                                 |
|                                                                             |                                                                                                                                   | Civil Litigation                                                |                      | Determine when someone was home or at a different location.                                                                                                                                                                                                   |
|                                                                             |                                                                                                                                   | PEV Lessor                                                      |                      | Verify a lessee’s compliance regarding the mileage of a lease agreement.                                                                                                                                                                                        |
| Identifies individual meters or customer-owned equipment and capabilities.  | *Identify Household Appliances*  
Identifying information (such as a MAC address); directly reported usage information provided by “Smart” appliances.  
Data revealed from compromised smart meter, HAN, or other appliance. | Utilities                                                                 | Primary               | Load monitoring and forecasting; efficiency analysis and monitoring; reliability; demand response; distributed energy resource management; emergency response.                                                                                                         |
|                                                                             |                                                                                                                                   | 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. |
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 that some insurance companies, employers, newspapers (when regarding public figures), civil litigants, and others could be interested in. Most directly, specific medical devices may be uniquely identified through serial numbers or MAC addresses, or may have unique electrical signatures; either could indicate that the resident suffers from a particular disease or condition that requires the device.

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. Electricity use could also reveal how much the resident sleeps and whether he gets up in the middle of the night. Similarly, appliance usage data could indicate how often

---


71 Elias Quinn mentions an Alabama tax provision that requires obese state employees to pay for health insurance unless they work to reduce their body mass index. Elias Quinn, Privacy and the New Energy Infrastructure, Feb. 2009 (draft) 31, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731. He suggests that Smart Grid data could be used to see how often a treadmill was being used in the home.

72 Ann Cavoukian, Jules Polonetsky, and Christopher Wolf, Privacy by Design, SmartPrivacy For the Smart Grid: Embedding Privacy into the Design of Electricity Conservation 11 (Nov. 2009), available at
meals are cooked with the microwave, the stove, or not cooked at all, as well as implying the frequency of meals.73 Many of the parties listed in the “Potential Privacy Impacts” table (Table 3-3) will not be interested in the health of the resident and will wish to use the data for purposes such as efficiency monitoring, but some parties may be interested in the behavioral assumptions Smart Grid entities could make with Smart Grid data.

3.6.2 Wireless Access to Smart Grid Meters and Secondary Devices

Future designs for some smart meters and many secondary devices (e.g., appliances and smaller devices) may incorporate wireless enabled technology to collect and transmit energy usage information for homes or businesses.74 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 have privacy protection.75 If in the future wireless technology is used to transmit aggregate home or business energy consumption information for a unique location or dwelling, then that usage data, prior to sufficient aggregation to protect privacy, should also be protected from unauthorized use, modification or theft.76 There are well known vulnerabilities related to wireless sensors and networks,77 and breaches of wireless technology.78 For example, “war driving” is a popular technique used to locate, exploit, or attack insufficiently protected wireless systems.79 Readily available portable computing devices are used to detect signals emanating from wireless technology.

http://www.ipc.on.ca/images/Resources/pbd-smartpriv-Smart Grid.pdf (describing the types of information that could be gleaned from combining PII with granular energy consumption data).

73 Id. at 11.


75 See, Table 3-2 Potential Privacy Concerns and Descriptions.

76 Data aggregation was addressed in the final HIPAA rule. See, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt. There may also be efficiencies that can be gained by the Smart Grid when aggregating data from transmission and processing that save money for utilities. (See, http://portal.acm.org/citation.cfm?id=1269968). This may create a greater incentive to aggregate data. If this is the case then proper aggregation to protect PII or sensitive data should be incorporated into the plan for data aggregation.


78 Id.

3.6.3 **Commissioning, Registration, and Enrollment for Smart Devices**

This section describes a method for implementing demand response using load control through an energy management system linked to a utility or a third party service provider offering remote energy management. As explained in Section 3.7, it is possible to protect customer privacy by implementing demand response without a direct data connection between the energy service provider and home devices.

To create a home area network, devices must, at a minimum, scan for networks to join, request admission, and exchange device parameters. This initial process is called “commissioning” and allows devices to exchange a limited amount of information (including, but not limited to, network keys, device type, device ID, and initial path) and to receive public broadcast information. This process is initiated by the “installer” powering-on the device and following the manufacturer’s instruction. Once a HAN device has completed the commissioning process it may go through an additional process called “registration.”

The registration process is a further step involving “mutual authentication” and authorizing a commissioned HAN device to exchange secure information with other registered devices and with a smart energy industrial provider. Registration creates a trust relationship between the HAN device and the smart energy industrial provider and governs the rights granted to the HAN device. This process is more complex than commissioning and requires coordination between the installer and the service provider. In some jurisdictions commissioning and registration are combined into one process called “provisioning.”

The final process is “enrollment.” This process is only applicable 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 his 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 customer 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.

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.

---

80 The first four paragraphs of this section are taken from OpenHAN v1.95:
Determining how the registration information is used, where it is stored, and with whom it is shared.

3.6.4 Smart Grid Data Accessibility via the Public Internet

The Smart Grid has the capability to allow users to interact with their electricity usage information in innovative ways, including via the Internet. Correspondingly, the transmission or publication of Smart Grid data via the Internet raises privacy challenges. Internet communications are generally unsecure unless those publishing the information take steps to protect the content against unauthorized interception, manipulation, or other compromises. Moreover, users do not always have complete knowledge of, or control over, how their data will be used.

For example, a social networking application may allow electricity consumers to monitor energy usage via cell phones, personal digital devices, and social networking pages. Social networking service providers are not regulated and have routinely changed user privacy settings to share more information than a user may have originally intended to share. Should such an unexpected change in privacy settings occur, a user's Smart Grid data may become publicly viewable by anyone and even indexed by search engines. Users of social networking applications that monitor electricity usage should receive adequate, publicly available education that demonstrates how use of these applications may allow access, by third parties or the public, to a great amount of information, potentially more than just electricity usage information.

This example is one of many possible data privacy issues confronted by the interaction of the Internet with Smart Grid technology. Considering the broad scope of this topic, more research is needed to fully explore the vast privacy implications.

3.6.5 Smart Grid Data Access by Third Parties

The Smart Grid may increase the frequency and detail of electricity consumption information on private homes and businesses. The electricity consumption data that is collected, retained, and transmitted over Smart Grid systems may be of interest to third parties. Third parties can include legitimate businesses with agreements with energy consumers to assist them in better managing energy consumption, but can also include thieves seeking to abuse or misuse data.

There are three privacy challenges presented by third party access to Smart Grid information—

---

81 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.

82 See http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

83 See http://www.cs.virginia.edu/felt/privacy/

1. That companies representing themselves as customer electricity management services are what they represent themselves to be;\textsuperscript{85}
2. What consumers are told about how their information will be used is true;\textsuperscript{86}
3. Party access to electricity usage data is being used solely for the purpose of managing electricity usage.

An effective full suite of FIPs protections is necessary for consumer privacy enforcement.

Authorized third parties may be interested in using data collected through the Smart Grid. The real-time data streaming capabilities of the Smart Grid may be attractive to large appliance manufacturers, marketers interested in usage information on utility or non-utility dependent small appliances, devices, or other consumer products.\textsuperscript{87} Unauthorized third parties will likely also be interested in misusing Smart Grid data for many reasons from theft of physical property, identity theft schemes, or surveillance of residences or businesses. E-mail “pharming” and “phishing” attacks have been successfully used by Internet thieves in tricking consumers into divulging personal information to thieves who use the information for an array of swindles and thefts. Pharming involves manipulation of stored search engine information housed on personal computing devices to redirect customers away from legitimate sites to fake e-locations. Phishing involves sending communications that appear to originate from a legitimate company or business. Once the message is opened it may download spyware or damaging software onto the computing device of the unsuspecting customer.

Companies have strongly relied upon “Notice and Choice” to gain customer consent for data collection, retention, and use. The marketing materials may promote lower energy bills through better management of energy consumption. However, the details of service agreements or “click-through” agreements of services offered solely over the Internet might contain more uses for data

\textsuperscript{85} Federal Trade Commission (FTC), Press Release, FTC Launches Redress Program for ChoicePoint Identity Theft Victims, (“Last year, ChoicePoint, a company that compiles and sells personal information, announced that it had sold information about many consumers to people who turned out to be identity thieves. The FTC, the nation’s consumer protection agency, investigated the ChoicePoint security breach and alleged that, in some cases, these sales resulted in identity theft,”) available at http://www.ftc.gov/opa/2006/12/choicepoint.shtm; FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress,” available at http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

\textsuperscript{86} FTC, Complaint “In the Matter of SEARS HOLDING MANAGEMENT CORPORATION” Docket No. C-4264, (“3. From on or about April 2007 through on or about January 2008, SHMC disseminated or caused to be disseminated via the Internet a software application for consumers to download and install onto their computers (the “Application”). The Application was created, developed, and managed for respondent by a third party in connection with SHMC’s “My SHC Community” market research program. 4. The Application, when installed, runs in the background at all times on consumers’ computers and transmits tracked information, including nearly all of the Internet behavior that occurs on those computers, to servers maintained on behalf of respondent. Information collected and transmitted includes: web browsing, filling shopping baskets, transacting business during secure sessions, completing online application forms, checking online accounts, and, through select header information, use of web-based email and instant messaging services,”) available at http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

than energy management. 88 Simple notice is not enough to assure electricity consumer privacy protection. There are particular challenges for reliance upon notice and consent in online agreements. A survey of California consumers showed that they fundamentally misunderstand their online privacy rights. 89

There are added complications for consent in online click-through applications or agreements because it will be difficult to assure solely through online means that the person requesting the third party energy management service is authorized to do so. For example, if application information for third party service seeks basic application information such as home address, utility account number, or name, this information would be found on a monthly bill, which is often discarded as trash. Verifying that the legitimate electricity customer is the one requesting service may require additional steps by utilities independent of the third party service provider. In addition, users routinely click through notices. The Pew Internet and American Life Project found that 73% of users do not always read agreements, privacy statements or other disclaimers before downloading or installing programs. Further, online businesses routinely change terms of service and privacy policy without giving notice to consumers. 90

Third party customer energy use sharing agreements may cause customers confusion regarding the source of data misuse or abuse should it occur.

3.7 MITIGATING PRIVACY CONCERNS WITHIN THE SMART GRID

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

Where there is an operational need for information, controls should be implemented to ensure that data is collected only where such a need exists. Organizations will benefit by developing policies to determine the customer and premises information that should be safeguarded and how that information should be retained, distributed internally, shared with third parties and secured against breach. As noted in other parts of this report, training employees is critical to implementing this policy. Similarly, Smart Grid services recipients should be informed as to what information the organization is collecting and how that information will be used, shared and secured. Service recipients may also need the ability to inspect collected information for accuracy and quality, as recommended in the privacy principles described in the PIA material (subsection 3.4.2).

88 David Vladeck, Privacy: Where do we go from here?, Speech to the International Conference on Data Protection and Privacy Commissioners, Nov. 6, 2009, (“[The notice and consent model] may have made sense in the past where it was clear to consumers what they were consenting to, that consent was timely, and where there would be a single use or a clear use of the data. That’s not the case today. Disclosures are now as long as treatises, they are written by lawyers—trained in detail and precision, not clarity—so they even sound like treatises, and like some treatises, they are difficult to comprehend if they are read at all. It is not clear today that consent today actually reflects a conscious choice by consumers,”) available at http://ftc.gov/speeches/vladeck/091106dataprotection.pdf

89 Joseph Turow, et al., Consumers Fundamentally Misunderstand the Online Advertising Marketplace, available at http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf

Existing business rules, standards, laws, and regulations previously considered applicable to other sectors of the economy might be usable as models to provide protection against the Type II areas of concern described earlier (subsection 3.6, Table 3-2). However, because of the current technology used for the collection of the data, Type I concerns may require new rules for business standards or regulation.

Many of the concerns relating to Smart Grid and privacy may be addressed by limiting the information required from an operational standpoint. For example, many existing implementations of demand response use direct load control, where the utility has a communications channel to thermostats, water heaters, and other appliances at customer premises. Although most direct load control today is one-way, if two-way communications are implemented, the pathway from the customer may allow granular monitoring of energy consumption by appliance. This direct monitoring may provide more accurate load management, but could also pose certain privacy risks.

There are other methods that use demand response for distributed load control where the utility or third party energy service provider delivers pricing and energy data to a customer Energy Management System (EMS) through a gateway. This gateway acts as a line of demarcation between the supplier and the customer, while intelligent appliances and/or the customer EMS use this pricing and energy information to optimize energy consumption according to customer preferences. With the insertion of a gateway and local intelligence, any feedback to the utility could be load control results for the entire household, rather than by appliance. To mitigate privacy concerns, these results need to be averaged over a long enough time interval to prevent pattern recognition against known load profiles, as explained in Section 3.3.6. Thus, it is possible to protect customer privacy at a macro level by choosing a system design that minimizes frequent access to granular data from outside the customer site.

3.7.1 Use Case Mitigation Studies

Whereas PIAs provide an excellent means of identifying privacy risks, privacy use cases can be excellent tools for determining the specific steps to take to mitigate privacy risks in ways that are reasonable for the organization; not only for mitigating risks discovered during PIAs, but also for mitigating the generally known risks involved with common business activities that involve personal information. These generally known risks can be represented by common privacy use cases. With heavy reliance upon technology and information sharing, addressing privacy risks must be part of the business model today, and consideration of privacy impacts should be part of everyday business activities. Privacy use cases can provide the engineers and architects of systems and processes the guidance and information necessary for building privacy controls into systems and processes during their daily activities. Further discussion of this need to build privacy protections into systems and processes, along with the resulting benefits, is provided within the “Privacy By Design” methodology.91

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

---

91 “Privacy By Design” is a set of seven high-level concepts, created by Ontario Privacy Commissioner Ann Cavoukian, for organizations to follow to help ensure they establish and build privacy controls within their business processes. See more about the Privacy By Design concepts at [http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf](http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf).
components to determine the privacy concerns that exist within their scope of Smart Grid use and participation. Privacy use cases may be utilized to represent generalizations of specific scenarios within the Smart Grid that require interoperability between systems and Smart Grid participants in support of business processes and workflow. Through structured and repeatable analysis, business use cases can be elaborated upon as interoperability/technical privacy use cases to be implemented by the associated entities within the Smart Grid. The resulting details will allow those responsible for creating, implementing, and managing the controls that impact privacy to do so more effectively and consistently.

3.7.2 Privacy Use Case Scenarios

The privacy subgroup spent several months creating a few different methods for expanding the existing NIST collection of use cases to include consideration of privacy concerns. When considering which set of FIPs to use for creating privacy use cases, it was decided to use the OECD Privacy Guidelines for the following reasons—

- They are long-established and widely recognized,
- They are freely available, and
- They are straightforward concepts that will be more easily and consistently utilized when building privacy controls into processes.

The larger set of amalgamated principles used to conduct the Smart Grid PIA were chosen because they better served the purposes of identifying where, within an identified system or process, the most comprehensive set of privacy concerns exist. Typically, PIAs are performed by a specific individual or specialized group within an organization, and the PIAs look at a broader scope within a system or process and go less in-depth than a privacy use case.

Privacy use cases are typically utilized by a broader community and are repeatedly used to examine a specific, narrow scope. By keeping the privacy use case process limited to one set of accepted privacy principles such as the OECD Privacy Guidelines it will be simpler and more feasible for the privacy use cases to be consistently used and applied by the broader community.

Appendix B contains the description of the activities the privacy subgroup took for creating privacy use cases. The privacy subgroup drafted multiple privacy use cases. The following are included as examples—

4. Landlord with Tenants scenarios
5. A PEV General Registration and Enrollment Process scenario

While the privacy subgroup created a few privacy cases, work needs to continue to finish developing a more comprehensive set of privacy use cases for publication in a subsequent version.

While producing the sample privacy use cases drafts, the privacy subgroup established many recommendations based upon the work that was completed. These include:

---

92 See the collection of use cases the Privacy Group considered and chose representative use cases from at [http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases](http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases).
• Expanding the current collection of use cases to cover all Smart Grid entity types in addition to utilities (regulated or not) that will offer Smart Grid and smart device services.
• Including a broader list of individual data subjects about whom the Smart Grid, smart meters, and smart devices will generate additional personal information.
• Including within use cases, where appropriate and feasible to allow Smart Grid goals and processes to be met, a method for individuals to turn off/on certain smart meter and smart devices collection of personal information.

The work done so far on creating privacy use cases has only begun to document the functions that need to be implemented to ensure privacy is protected in Smart Grid operations. The privacy subgroup recommends ongoing development of a comprehensive set of use cases for privacy.

### 3.8 SMART GRID PRIVACY SUMMARY AND RECOMMENDATIONS

#### 3.8.1 Summary

Based upon the work and research done over the past year, the privacy subgroup reached the following conclusions:

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

2. New Smart Grid technologies, particularly smart meters, smart appliances, and similar types of endpoints, may create new privacy risks and concerns that may not be addressed adequately by the existing business policies and practices of utilities and third party Smart Grid providers.

3. Utilities and third party Smart Grid providers need to follow recognized privacy practices to effectively safeguard Smart Grid personal information and customer privacy.

#### 3.8.2 Recommendations

The challenge ahead is to create a compelling, transparent Smart Grid Fair Information Principles program that individuals trust enough to utilize the Smart Grid so that the energy industry thrives and innovation occurs. This will only happen when effective and transparent privacy practices are consistently implemented, followed, and enforced within the Smart Grid. To create this transparency and obtain the trust of Smart Grid participants—and based on the conclusions and the details of the associated findings—recommendations were made throughout this chapter for all entities that participate within the Smart Grid. A summary listing of all these recommendations includes:

1. Conduct a PIA upon making the decision to deploy and/or participate in the Smart Grid to identify risks to the personal information Smart Grid entities collect, process, store, and otherwise handle, along with determining appropriate risk mitigation activities. Smart Grid entities can refer to the methodology followed by the privacy subgroup, as described
• Conduct an initial PIA to identify existing privacy risks and establish a baseline privacy posture measurement.

• Conduct subsequent PIAs when major changes occur within the organization, systems, or applications; when new laws and regulations are put into effect that provide requirements for how Smart Grid data is used; and at any other time an event occurs that impacts how the Smart Grid entity does business, such as following an information security incident involving personal information.

2. Develop and formally document privacy policies and practices that are drawn from the full set of OECD Privacy Principles. In particular the privacy subgroup recommends the following practices based on the Principles:

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

• **Notice and Purpose.** An organization should provide customers with meaningful, clear, and full notice in advance of the collection, use, retention, or sharing of energy usage data and personal information. Such notice should provide a detailed description of all purposes for which customer data will be used, including any purposes for which affiliates and third parties will use the data. The notice should also include how long the data will be maintained by the organization and which third parties the data will be shared with. Clear, full, and accurate notice prior to data collection is essential to enabling other principles.

• **Choice and Consent.** An organization should clearly, fully, and accurately describe the choices available to individuals, and to the extent practicable, obtain explicit approval for the collection and use of their personal information. Customers should have the option to forgo data collection and services that are not related to the core services provided by the organization.  

• **Collection and Scope.** Only personal information that is required to fulfill the stated purpose specified under the Notice and Purpose principle should be collected. Treatment of the information should conform to these privacy principles.

• **Use and Retention.** Information should only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. Personal information should be aggregated or anonymized wherever possible to limit the potential for revealing private information. Personal information

---

93 For example, while they may not have a choice about collection necessary for load balancing, electricity customers should have the option to prohibit utilities from collecting information about their appliances for marketing uses.
• **Individual Access.** Organizations should provide a process whereby individuals may to ask to see their corresponding personal information and to correct inaccuracies. Individuals should be informed about parties with whom personal information has been shared.

• **Disclosure and Limiting Use.** Personal information should be used only for the purposes for which it was collected. Personal information should not be disclosed to any other parties except those identified in the notice for purposes identified in the notice, or with the explicit consent of the service recipient. Unless disclosure is compelled by a subpoena, warrant, or court order, organizations should seek prior customer approval for disclosure of customer data to third parties.

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

3. Develop a comprehensive set of privacy use cases that will help utilities and third-party Smart Grid providers to rigorously track data flows and the privacy implications of collecting and using data, and help the organization to address and mitigate the associated privacy risks within common technical design and business practices.

4. Educate the public about the privacy risks within the Smart Grid and what they as consumers can do to mitigate them.

5. Share information concerning solutions to common privacy-related problems with other Smart Grid market participants.

6. Manufacturers and vendors of smart meters, smart appliances, and other types of smart devices, should collect only the energy and personal data necessary for the purposes of the smart device operations. The defaults for the collected data should be established to use and share the data only as necessary to allow the device to function as advertised.

Given these realities, findings, and recommendations, the privacy subgroup hopes that the information contained in this chapter will serve as a useful guide and reference for the wide variety of Smart Grid domain players, policymakers, and lawmakers who have or may in the future, have responsibility for consumer energy consumption data.
# APPENDIX A:
## STATE LAWS – SMART GRID AND ELECTRICITY DELIVERY REGULATIONS

<table>
<thead>
<tr>
<th>State</th>
<th>Code Topic and Links</th>
</tr>
</thead>
</table>
| Alabama        | Title 37 Public Utilities  
Private Contractor providing electricity service Section 37-4-30,  
Electric cooperatives empowered to furnish telephone service. Section 37-6-41,  
Cooperatives authorized to supply electrical energy or telephone service or both. Section 37-6-45  
http://www.legislature.state.al.us/CodeofAlabama/1975/coatoc.htm |
| Alaska         |                                                                                                                                                    |
| Arizona        | 42-5063  
Definition of Utility - Providing to retail electric customers ancillary services,  
electric distribution services, electric generation services, electric transmission  
services and other services related to providing electricity.  
Customer Protection against unfair and deceptive practices. It has very good consumer protection language  
http://law.justia.com/arizona/codes/title30/00806.html  
Statute 30-803 Competition in retail supply of electricity; open markets  
http://law.justia.com/arizona/codes/title30/00803.html |
| Arkansas       |                                                                                                                                                    |
| California     | General Provisions and Definitions  
http://law.justia.com/california/codes/puc/201-248.html  
Distributed Energy Resources http://law.justia.com/california/codes/puc/353.1-353.15.html  
Privacy Protection of customer data  
http://law.justia.com/california/codes/puc/2891-2894.10.html |
| Colorado       | Article 25 Public Utility Commission Power to regulate utilities  
http://law.justia.com/colorado/constitution/cnart25.html |
| Connecticut    | Chapter 98 http://search.cga.state.ct.us/dtsearch_pub_statutes.html Sec. 7-148ee. Establishment of corporation to manufacture, distribute, purchase  
or sell electricity, gas or water.  
Chapter 101 http://search.cga.state.ct.us/dtsearch_pub_statutes.html Municipal  
Gas and Electric Plant  
All regulatory measures under Chapter 101  
http://search.cga.state.ct.us/dtsearch_pub_statutes.html |
| Delaware       | Title 26 Public Utilities  
http://delcode.delaware.gov/title26/index.shtml#TopOfPage |
<p>| District of Columbia | Title 34 |
| Florida        | Title 27 Regulated Utilities |</p>
<table>
<thead>
<tr>
<th>State</th>
<th>Code Topic and Links</th>
</tr>
</thead>
</table>
| Georgia     | Article 2, 6  
| Hawaii      | §269-16 Regulation of utility rates; ratemaking procedures.  
http://www.capitol.hawaii.gov/hrscurrent/Vol05_Ch0261-0319/HRS_0269-0016.htm                                                                 |
| Idaho       | Title 61  
http://www.legislature.idaho.gov/idstat/Title61/T61.htm                                                                                             |
| Illinois    | Chapter 220  
| Indiana     | Title 8  
http://www.in.gov/legislative/ic/code/title8/                                                                                                       |
| Iowa        |                                                                                                                                                    |
| Kansas      | Chapter 66-101  
http://www.kslegislature.org/legsrv-statutes/statutesList.do  
66-1901-66-1903  
http://www.kslegislature.org/legsrv-statutes/statutesList.do                                                                                     |
| Kentucky    | Title 24 Public Utilities Generally  
http://www.lrc.ky.gov/KRS/278-00/CHAPTER-HTM                                                                                                          |
| Louisiana   | Louisiana Public Utilities Definition  
http://www.legis.state.la.us/lss/lss.asp?doc=99873  
http://www.legis.state.la.us/lss/lss.asp?doc=99891  
http://www.legis.state.la.us/lss/lss.asp?doc=99803  
http://www.legis.state.la.us/lss/lss.asp?doc=104770                                                                                                    |
| Maine       | Public Utilities  
http://www.mainelegislature.org/legis/statutes/35/title35ch0sec0.html                                                                                   |
| Maryland    | Statute 1-101 Definitions  
http://mlis.state.md.us/asp/statutes_Respond2.asp?article=gpu&section=1-101  
§ 6-109. Duty of owner, lessee, or user of equipment.  
§ 7-306. Net energy metering.  
§ 7-509. Electric company’s authority to regulate.  
Title 6. High voltage lines  
Title 7. Gas, electric, and water companies                                                                                                               |
| Massachusetts |                                                                                                                                                    |
| Michigan    | Chapter 460  
| Minnesota   | Chapter 216-217  
<p>|             | Chapter 453 Municipal Electric Power                                                                                                                  |</p>
<table>
<thead>
<tr>
<th>State</th>
<th>Code Topic and Links</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chapter 455 Electric Light and Power Plants</td>
</tr>
<tr>
<td>Missouri</td>
<td></td>
</tr>
<tr>
<td>Montana</td>
<td>Title 69 Public Utilities and Carriers</td>
</tr>
<tr>
<td></td>
<td>Title 69 Chapter 3 Regulation of Public Utilities</td>
</tr>
<tr>
<td></td>
<td><a href="http://data.opi.state.mt.us/bills/mca_toc/69_3.htm">http://data.opi.state.mt.us/bills/mca_toc/69_3.htm</a></td>
</tr>
<tr>
<td>Nebraska</td>
<td></td>
</tr>
<tr>
<td>Nevada</td>
<td>Title 58 Chapter 701</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.leg.state.nv.us/NRS/NRS-701.html">http://www.leg.state.nv.us/NRS/NRS-701.html</a></td>
</tr>
<tr>
<td></td>
<td>Renewable Energy Program</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.leg.state.nv.us/NRS/NRS-701B.html">http://www.leg.state.nv.us/NRS/NRS-701B.html</a></td>
</tr>
<tr>
<td></td>
<td>Chapter 703 Public Utility Commission</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.leg.state.nv.us/NRS/NRS-703.html">http://www.leg.state.nv.us/NRS/NRS-703.html</a></td>
</tr>
<tr>
<td></td>
<td>Regulation of Public Utilities</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.leg.state.nv.us/NRS/NRS-704.html">http://www.leg.state.nv.us/NRS/NRS-704.html</a></td>
</tr>
<tr>
<td></td>
<td>Utilities Owned by Local Government</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.leg.state.nv.us/NRS/NRS-710.html">http://www.leg.state.nv.us/NRS/NRS-710.html</a></td>
</tr>
<tr>
<td>New Hampshire</td>
<td>Statutes</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.gencourt.state.nh.us/rsa/html/indexes/indexresults.asp">http://www.gencourt.state.nh.us/rsa/html/indexes/indexresults.asp</a></td>
</tr>
<tr>
<td></td>
<td>Definitions</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.gencourt.state.nh.us/rsa/html/xxxiv/374-a/374-a-1.htm">http://www.gencourt.state.nh.us/rsa/html/xxxiv/374-a/374-a-1.htm</a></td>
</tr>
<tr>
<td></td>
<td>Private Generation and Sell of Electricity</td>
</tr>
<tr>
<td></td>
<td>Customer Defined</td>
</tr>
<tr>
<td></td>
<td>Public Utility Defined</td>
</tr>
<tr>
<td>New Jersey</td>
<td></td>
</tr>
<tr>
<td>New Mexico</td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td>Electric Utility Cooperatives and Corporations</td>
</tr>
<tr>
<td></td>
<td><a href="http://public.leginfo.state.ny.us/menugetf.cgi?COMMONQUERY=LAWS">http://public.leginfo.state.ny.us/menugetf.cgi?COMMONQUERY=LAWS</a></td>
</tr>
<tr>
<td></td>
<td>Title 2 Article 5 Public Utility Commission</td>
</tr>
<tr>
<td></td>
<td><a href="http://public.leginfo.state.ny.us/menugetf.cgi?COMMONQUERY=LAWS">http://public.leginfo.state.ny.us/menugetf.cgi?COMMONQUERY=LAWS</a></td>
</tr>
<tr>
<td>North Carolina</td>
<td></td>
</tr>
<tr>
<td>North Dakota</td>
<td>Title 49 Public Utilities</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.legis.nd.gov/cencode/t49.html">http://www.legis.nd.gov/cencode/t49.html</a></td>
</tr>
<tr>
<td>Ohio</td>
<td>Chapter 743 Utilities – Electric; Gas; Water</td>
</tr>
<tr>
<td></td>
<td><a href="http://codes.ohio.gov/orc/743">http://codes.ohio.gov/orc/743</a></td>
</tr>
<tr>
<td>Oklahoma</td>
<td></td>
</tr>
<tr>
<td>Oregon</td>
<td>Title 57 Utility Regulation</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.leg.state.or.us/ors/756.html">http://www.leg.state.or.us/ors/756.html</a></td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>Title 66</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>Title 39 Public Utilities and Carriers</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.rilin.state.ri.us/Statutes/TITLE39/INDEX.HTM">http://www.rilin.state.ri.us/Statutes/TITLE39/INDEX.HTM</a></td>
</tr>
<tr>
<td>State</td>
<td>Code Topic and Links</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>South Carolina</td>
<td>Article 3 Electric Systems <a href="http://www.scstatehouse.gov/coderegcs/c103.htm">http://www.scstatehouse.gov/coderegcs/c103.htm</a></td>
</tr>
<tr>
<td></td>
<td>Chapter 40 Publicly Owned <a href="http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.40.htm">http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.40.htm</a></td>
</tr>
<tr>
<td></td>
<td>Chapter 41 Cooperatives <a href="http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.41.htm">http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.41.htm</a></td>
</tr>
<tr>
<td></td>
<td>Chapter 43 Access to Broadband <a href="http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.43.htm">http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.43.htm</a></td>
</tr>
<tr>
<td>Utah</td>
<td>Title 54 Public Utilities <a href="http://le.utah.gov/~code/TITLE54/TITLE54.htm">http://le.utah.gov/~code/TITLE54/TITLE54.htm</a></td>
</tr>
<tr>
<td>Vermont</td>
<td>Title 56 Section 580 Transmission and distribution of electricity <a href="http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+56-580">http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+56-580</a></td>
</tr>
<tr>
<td></td>
<td>Definitions <a href="http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+56-265.1">http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+56-265.1</a></td>
</tr>
<tr>
<td>West Virginia</td>
<td>Chapter 196 Regulation of Public Utilities <a href="http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&amp;fn=default.htm&amp;d=index&amp;jd=top">http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&amp;fn=default.htm&amp;d=index&amp;jd=top</a></td>
</tr>
<tr>
<td></td>
<td>Utility service for persons who are victims of Identity Theft <a href="http://www.legis.state.wi.us/statutes/Stat0196.pdf">http://www.legis.state.wi.us/statutes/Stat0196.pdf</a></td>
</tr>
<tr>
<td>Wyoming</td>
<td>Title 37 Public Utilities</td>
</tr>
</tbody>
</table>
APPENDIX B:
PRIVACY USES CASES

The privacy subgroup—

- Reviewed a large number of existing Smart Grid use cases;\(^{94}\)
- Identified the privacy gaps within and among those use cases;
- Developed augmented use cases for privacy, using the traditional format used by the CSWG\(^ {95}\), the OECD privacy principles, and Version 2.0 of the International Security, Trust & Privacy Alliance (ISTPA) Privacy Management Reference Model;\(^ {96}\) and
- Summarized the key findings and observations from the collection of all the privacy use cases created.

B.1 USE CASE INVENTORY, CONSOLIDATION AND GAP ANALYSIS

The privacy subgroup developed a consolidated matrix\(^ {97}\) of the existing use cases, by like topic, then looked for use cases that could represent common Smart Grid scenarios involving personal information.

The use cases were selected from several existing sources, including but not limited to IntelliGrid, Electric Power Research Institute (EPRI), and Southern California Edison (SCE).

Review of this collection of use cases revealed the following:

- The existing use cases relate to utilities but not to the third parties that will also be part of the Smart Grid.
- It is not clear that the current use cases include non-regulated (e.g., third parties) Smart Grid entities or services that do not operate through the smart meter. All of the use cases reviewed require registration with a regulated Smart Grid entity and operation through the smart meter. More use cases are needed to make the set available comprehensive.
- The use cases represent situations where data is captured from not only utilities, but also from smart devices, such as a HAN or a PEV using a different plug.
- All of the use cases—
  - Referred to an individual customer, even though the information collected could be from an individual, a dwelling with multiple individuals, or business other than the

---

\(^{94}\) See the collection of use cases that the Privacy Group considered and chose representative use cases from at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases.

\(^{95}\) See Appendix A in Draft 2 of NISTIR 7628, at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628Feb2010/DRAFT2_NISTIR_7628_Jan-31-2010_clean.pdf, to see how the security groups involved in this research formatted their use cases.

\(^{96}\) Developed by the International Security, Trust & Privacy Alliance (ISTPA) in 2009;

\(^{97}\) See the collection of use cases that the Privacy Group considered and chose representative use cases from at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases.
customer paying the Smart Grid entity bill. However, information within the Smart Grid could be personal information about a tenant, a household member, a visitor, a patient, an employee that the customer may not have the authority to grant permission to collect, and so on.

- Referred to a customer and the Smart Grid entity, even though the information collected could be from multiple individuals and could go to many entities outside of the utility.

- Reviewed assumed that if the service goes “through” the Smart Grid it has to involve the utility. There is no pass-through capability that allows an individual or business entity to enter into an agreement with a third party using Smart Grid personal information and additional personal information generated by the smart device that travels over the grid channels.

- Assume that the Smart Grid entity can know what electronic devices are on/off/running at a premise and do not address a privacy option that could be turned on/off at some level by the individual at the premise.

• None of the use cases reviewed—

  - Made mention of a privacy policy being disseminated and being agreed to by customers.

  - Specified privacy functionality.

  - Depicted a non-regulated entity (e.g., third parties) offering a service directly to an individual or business via a smart meter.

  - Specified smart devices that communicated outside of the Smart Grid, directly with the Internet or otherwise.

B.2 INCORPORATING PRIVACY INTO EXISTING SMART GRID USE CASES

Based upon the findings the privacy subgroup recommends the following guidelines for improving upon use cases to address privacy issues—

• Add on to the existing use cases by including privacy functionality to the scenarios.

• Include information within the use cases for the existence of such things as privacy policies, training, and so on as indicated within the PIA recommendations.

• Include within the use case scenarios (1) a relationship with the utility, (2) a joint relationship with the Smart Grid utility and non-regulated entity, and (3) a relationship solely with a non-regulated entity.

• Create use cases that—

  - Include third parties that will be part of the Smart Grid.
- Include privacy options where individuals within service locations can turn on and off the ability for utilities to detect electronic devices that are using energy.

- Depict a non-regulated entity offering a service directly to an individual or business via the smart meter.

- Depict scenarios that involve smart devices and other entities within the Smart Grid communicating directly with the Internet and other non-Smart Grid entities.

- Depict groups of individuals as being the customer, or individuals at service locations who are not the entities that pay for the services. (e.g., renters that pay utilities to the landlord, not the utility)

- Include the Smart Grid entity making an agreement with a third party and the third party making the agreement with the individual or business entity, much like the iPhone model. In this model, the individual or business entity may or may not be the customer, but may be the owner of a smart device that communicates with the smart meter.

### B.3 Privacy Use Case Examples

This appendix contains the details for two example privacy use cases that were identified as examples to map to the OECD Privacy Guidelines privacy protection and fair information practices model. Each of the applicable principles is noted in the steps provided with each use case.

For reference while reviewing these privacy use cases, here is a summary of the OECD Privacy Guidelines:

1. **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except—
   - with the consent of the data subject; or
   - by the authority of law.

5. **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual Participation Principle**: An individual should have the right—
   a. To obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. To have communicated to him, data relating to him
      i. within a reasonable time;
      ii. at a charge, if any, that is not excessive;
      iii. in a reasonable manner; and
      iv. in a form that is readily intelligible to him;
   c. To be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and
   d. To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. **Accountability Principle**: A data controller should be accountable for complying with measures that give effect to the principles stated above.

**B.4 PRIVACY USE CASE #1: LANDLORD WITH TENANTS**

"Utility Use Case Landlord/Tenant enrolls in/uses/is billed by a Smart Meter Program. In this use case, the tenant has a PEV.

**B.4.1 Use Case Assumptions**

- The Landlord has an account with the utility for the smart meter. The Landlord pays for all electrical service at the Tenants’ premises except for the PEV.
- Each Tenant associated with a Smart Meter has the right to prevent the Landlord from obtaining detailed energy usage that would depict the presence of electrical devices in the unit as this would be an invasion of privacy.
- PEV Tenant has an account with utility and electrical service at a premise served by the utility.
- PEV and utility have communications capabilities, enabled by utility provided Energy Services Communication Interface (ESCI).
- The Tenant awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.
  - The utility offers PEV programs and services for its customers and will provide the necessary support processes for enrollment, communications, and billing
  - The Vehicle manufacturer would provide information to the customer about fuel and/or emission gains of the vehicles offered and promote the utility and convenience of connecting to the grid
• Utility maintains information on all Landlord’s Smart Meters and Tenant’s PEVs enrolled in the PEV programs, including demand side management programs, associated PEV IDs, Landlord IDs, and premise IDs. The Landlord is permitted detail reports, only if the Tenant allows such, even though the Landlord is paying for the electricity.

• For the purposes of this use case all of the ‘DEFINE’ Privacy Reference Model operational requirements have been established such that the Landlord and the Tenant have only to ‘SELECT’ their choices.

B.4.2 Step-by-Step Breakdown

Scenario: Landlord enrolls in the Smart Meter program. Tenants provide (or not) permission for Landlord to see detailed Smart Meter Reports and the Utilities Company turns on the service

This scenario describes the enrollment and initial usage of the Smart Meter Program.

Step 0.5 - The Landlord awareness of the utility and Smart Meter programs is prompted by both the utility providers and the Smart Meter manufacturers.

Step 1 - Landlord initiates request to enroll Smart Meter(s) in a Smart Meter Program by contacting Utility and provides Landlord, Tenant and Smart Meter information (i.e. Landlord Account information, Tenant associated with Smart Meter, SM ID, etc.). [Note: Landlord uses phone, Internet, or other communications channel.]

OECD Data Quality Principle: Collection of Personal data by the Landlord should be relevant to the purposes for which it will be used as stated by the Smart Meter provider.

Step 2 - Utility authenticates Landlord, Landlord account, and Premise information, and. collects Smart Meter information including SM ID and associated Tenant information

OECD Security Safeguards Principle: Utility must ensure proper authentication procedures are followed prior to creating a new account.

Step 3 - Utility presents Landlord with Smart Meter Program information and Smart Meter Program selections.

OECD Purposes Specification Principle: The collection of personal data should be specified by the Landlord to any Tenant and the subsequent use of the data limited to the fulfillment of those purposes

OECD Openness Principle: Utility makes available information collection and use policies to Landlord.

Step 4 - Landlord selects Smart Meter Program and Service Plan, sets Smart Meter program parameters. The Landlord and Smart Meter are now enrolled in a utility Smart Meter program.

Step 4.1 - Tenant initiates request to set up Smart Meter(s) preferences by contacting Utility and provides Landlord, Tenant and Smart Meter information (i.e. Landlord Account information, Tenant associated with Smart Meter, SM ID, etc.). [Note: Tenant uses phone, Internet, or other communications channel.]

OECD Openness Principle: Utility and Landlord make available information collection and use policies to tenant.

Step 4.2 - Utility authenticates Tenant, Landlord account, and Premise information, and collects Smart Meter information including SM ID and associated Tenant information.
**OECD Security Safeguards Principle:** Utility must ensure proper authentication procedures are followed by Landlord and Tenant prior to collection of Smart Meter information.

**Step 4.3** - Utility presents Tenant with Smart Meter Program information and Smart Meter Program selections.

**OECD Purpose Specification Principle:** Tenant should be informed of the purposes for which personal data are collected should be specified not later than at the time of collection and the use limited to the fulfillment of those purposes.

**OECD Use Limitation Principle:** Tenant personal data should not be disclosed, made available, or otherwise used for purposes other than those specified by the Tenant.

**Step 4.4** - Tenant selects Smart Meter Program and Service Plan, sets Smart Meter program parameters. The Landlord, Tenant and Smart Meter are now enrolled in a utility Smart Meter program.

**OECD Individual Participation Principle:** Utility must ensure proper procedures are followed for collection of Smart Meter information.

**Step 5** - Tenant uses electrical services at their premise location.

**Step 6** - Smart Meter and Energy Services Communications Interface (ESCI) initiate a secure communications session.

**OECD Security Safeguards Principle:** Utility must ensure communications channel over which information will flow is appropriately secured.

**Step 7** - Smart Meter ID is transmitted to ESCI.

**OECD Security Safeguards Principle:** Utility must ensure communications channel over which information will flow is appropriately secured.

**Step 8** - ESCI maintains communication session and security between Smart Meter and Utility. ESCI transmits request for validating Smart Meter ID to Utility, includes Premise ID.

**OECD Security Safeguards Principle:** Same as Step 6, plus ensuring smart meter ID matches account created.

**Step 9** - Utility identifies and authenticates Smart Meter ID and Premise ID.

**OECD Security Safeguards Principle:** Utility ensures receiving IDs are correct before beginning session.

**Step 10** - Utility transmits confirmation message via ESCI to Smart Meter indicating successful binding with premise ESCI. Confirmation message includes authentication parameters for Smart Meter. [Note: Authentication parameters would include utility rate program information.]

**OECD Security Safeguards Principle:** Utility ensures data is safeguarded

**Step 11** - Smart Meter receives confirmation message and sets authentication parameters.

**OECD Security Safeguards Principle:** Utility ensures data is safeguarded and only authorized access to the data is allowed

**Step 12** - Smart Meter transmits via ESCI message to Utility acknowledgement of receipt of valid confirmation message and setting of authentication parameters

**OECD Security Safeguards Principle:** Utility ensures data is safeguarded and provides security and authentication for access to the data
Step 13 - Utility transmits message via ESCI to discover EUMD at Tenant Premise; message includes authentication parameters for EUMD. [Note: Authentication parameters would include utility rate program information (e.g. interval size, etc.).]

OECD Security Safeguards Principle: Utility ensures data is safeguarded, data is correct and sent to valid Customer (Tenant)

Step 14 - EUMD receives discovery message and sets authentication parameters.
OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 15 - EUMD transmits via ESCI message to Utility acknowledgement of receipt of valid discovery message and setting of authentication parameters
OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 16 - ESCI transmits confirmation message to PEV indicating successful communication session binding of PEV to Utility, meaning that charging can proceed according to enrolled PEV program. [Note: Authentication between Utility and Smart Meter is now complete and the Smart Meter processing can proceed according to the enrolled Smart Meter program criteria]

OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 17 - Smart Meter prepares for collection of electrical usage based on Landlord-selected preferences, Tenant-selected preferences and enrolled Smart Meter program.
OECD Data Quality Principle: Utility ensures that meter collects only personal data relevant to the purposes for which the data is to be used and be accurate, complete and kept up-to-date.
OECD Purpose Specification Principle: Utility follows Tenant preferences regarding personal data collection and the subsequent limited use
OECD Use Limitation Principle: Utility maintains process so that personal data is not disclosed, made available or otherwise used for purposes other than those specified by the Tenant

Step 18 - Utility prepares for report of electrical usage based on Landlord-selected preferences, Tenant-selected preferences and enrolled Smart Meter program.
OECD Individual Participation Principle: Data and usage collection reports should be made available to Tenant according to their preferences
OECD Accountability Principle: Utility is held accountable for complying with data security and access requirements

B.5 PRIVACY USE CASE #2: PEV GENERAL REGISTRATION AND ENROLLMENT PROCESS

Customers are interested in fueling vehicles with electricity. Electric vehicles (EV), plug-in vehicles (PEV) and plug-in hybrid vehicles (PHEV) are emerging transportation options for consumers. Electric utilities desire to support these emerging loads with electricity at “off peak” times when energy costs are low and generation and power delivery assets are underutilized. PEV manufacturers are interested in working with utilities to develop customer rates/programs which could provide consumers with an increased incentive to purchase a PEV. To enable utility customer rates/programs specifically to customers with PEVs, the utility must offer special services for these customers. These services include the ability to enroll, register, and initially setup communications between a PEV and the utility (one-time setup), the ability to repeatedly re-establish communications for each PEV charging session (repeat communications/re-binding), the ability to provide PEV charging (and other) status information to
customer information channels (e.g. web, display devices), and the ability to correctly bill PEV customers according to their selected rates/programs.

The Utility may offer the Customer a PEV tariff that provides a low rate for off-peak charging and a higher rate for on-peak charging. The utility must provide services to support energy supplied to customer PEV. These services include enrollment into a PEV program, PEV communications session binding, PEV energy billing, and PEV information services. The utility will implement an enrollment system for Customers with a PEV including registration and commissioning. The utility’s Energy Services Communication Interface (ESCI) allows for the establishment of a communications session (communications binding), at a premise location each time a PEV plugs in for charging. Energy supplied to the PEV is reported to the utility for billing and presentation to the Customer. Information related to utility PEV programs, energy usage, and PEV charging status/information will be made available to the Customer for viewing via a website or other customer provided display equipment. This use case covers general information for the following five scenarios:

1. Enrollment Process to Time of Use (TOU) Program
2. Enrollment Process to Direct Load/Device Control (DDC) Program
3. Enrollment Process to Real Time Pricing (RTP) or Hourly/Periodic Pricing Program
4. Enrollment Process to Critical Peak Pricing (CPP) or Hourly/Periodic Pricing Program
5. Enrollment Process to Active Load Management Program

- These programs apply to routine or prearranged customer, vehicle usage and charging events.
- It is expected that the enrollment process would identify the customers normal charging pattern, specific details on the vehicle(s) operated that could be matched with anticipated load info to predict minimum effects on the grid.

**B.5.1 Use Case Assumptions**

- PEV Customer has an account with utility and electrical service at a premise served by the utility.
- PEV and utility have communications capabilities, enabled by utility provided Energy Services Communication Interface (ESCI).
- The customer awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.
  - The utility offers PEV programs and services for its customers and will provide the necessary support processes for enrollment, communications, and billing
  - The Vehicle manufacturers would provide information to the customer about fuel and/or emission gains of the vehicles offered and promote the utility and convenience of connecting to the grid
- Utility maintains information on all Customers and PEVs enrolled in the PEV programs, including demand side management programs, associated PEV IDs, customer IDs, and premise IDs
- EUMD function can be inclusively located anywhere in a zone from the PEV and the branch circuit panel connection.
- In the absence or failure of PEV-utility communications, or if PEV ID validation fails, PEV charging will always proceed; however, without the incentive rates and with all energy charges accruing to the premise customer according to the premise customer’s default rate/service plan.
• The actual PEV charging processes, including scenarios for intra-and inter-utility roaming, are covered in use case P2.

• End Use Measurement Device (EUMD) is always available for PEV charging. If not available, charging will proceed without incentive rates and with all energy charges accruing to the premise customer. This may or may not prevent certain charging status indicators/metrics being available to customer for presentation/display purposes.

• EUMD function can be inclusively located anywhere in a zone from the PEV and the branch circuit panel connection.

To allow for possibility of the EUMD being a part of/within the PEV, PEV is a sub-meter to the primary utility billing meter at any premise (as opposed to being a separate service account with dual meter socket adapter)

The PEV and Utility will communicate to implement one or more the previously described Utility programs

B.5.2 Step by Step Breakdown

Scenario: Customer enrolls in PEV program (Basic Enrollment) and completes initial setup for PEV–Utilities communications

This scenario describes the most common sequence (basic process) of the utility enrolling a PEV customer into a utility program/service specifically for customers with PEVs. As described in the main Narrative section, the customer is enrolling in a PEV program/service that may provide for the opportunity to fuel a vehicle at a lower cost during off-peak periods based on one of the utility programs enumerated in the main Narrative section. This scenario involves both enrollment of the PEV and steps needed to establish an initial communications session with the utility.

Step 0.5 - The customer awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.

Step 1 - Customer initiates request to enroll PEV in a PEV Program by contacting Utility and provides Customer and PEV information (i.e. Customer Account information, PEV ID, etc.). [Note: Customer uses phone, Internet, or other communications channel. Preference for PEV is PEV VIN #]

OECD Collection Limitation Principle: Utility collects data by action of the customer

Step 2 - Utility authenticates Customer, Customer account, and Premise information, and collects PEV information including PEV ID.

OECD Security Safeguards Principle: Customer Account data authenticated by Utility to establish identification for PEV

Step 3 - Utility presents Customer with PEV Program information and PEV Program selections.

OECD Purpose Specification Principle: Utility communications to Customer regarding data collection practices

Step 4 - Customer selects PEV Program and Service Plan, sets PEV program parameters (e.g., guest charging, allow roaming, etc.). The Customer and PEV are now enrolled in a utility PEV program.

OECD Individual Participation Principle: Customer confirms data collection arrangements with Utility
Step 5 - Customer connects at their premise location. [Note: The connection could be using either EVSE corset or Premise EVSE. In this scenario we will consider that PEV is connected through EVSE cordset]

Step 6 - PEV and Energy Services Communications Interface (ESCI) initiate a secure communications session. [Note: Implementation could have PEV or ESCI as initiator of session.]

**OECD Security Safeguards Principle:** Utility establishes secure interface and authenticates session for data collection

Step 7 - PEV ID is transmitted to ESCI. [Note: Unique PEV ID will ultimately support portability of charging, among other purposes.

**OECD Security Safeguard Principle:** Utility collects Customer data through PEV identification using secure interface and by rearranged process and procedure to secure the data

Step 8 - ESCI maintains communication session and security between PEV and Utility. ESCI transmits request for validating PEV ID to Utility, includes Premise ID.

**OECD Security Safeguard Principle:** Utility maintains secure interface to transmit data it has collected. Data is also validated according to Utility procedures

Step 9 - Utility identifies and authenticates PEV ID and Premise ID. [Note: PEV binds with utility]

**OECD Data Quality Principle:** Utility confirms identity and authenticates data per collection practices

Step 10 - Utility transmits confirmation message via ESCI to PEV indicating successful binding with premise ESCI. Confirmation message includes authentication parameters for PEV.

**OECD Security Safeguards Principle:** Utility communicates data through secure interface and confirms data transmission

Step 11 - PEV receives confirmation message and sets authentication parameters.

**OECD Security Safeguards Principle:** Utility confirms data transmission

Step 12 - PEV transmits via ESCI message to Utility acknowledgement of receipt of valid confirmation message and setting of authentication parameters.

**OECD Security Safeguards Principle:** Utility through secure interface confirms data transmission

Step 13 - Utility transmits message via ESCI to discover EUMD at Customer Premise; message includes authentication parameters for EUMD. [Note: Authentication parameters would include utility rate program information (e.g. interval size, etc.).]

**OECD Security Safeguards Principle:** Utility communicates data through secure interface and confirms data transmission

Step 14 - EUMD receives discovery message and sets authentication parameters.

**OECD Security Safeguards Principle:** Utility communicates data through secure interface and confirms data transmission

Step 15 - EUMD transmits via ESCI message to Utility acknowledgement of receipt of valid discovery message and setting of authentication parameters.

**OECD Security Safeguards Principle:** Utility communicates data through secure interface and confirms data transmission
Step 16 - ESCI transmits confirmation message to PEV indicating successful communication session binding of PEV to Utility, meaning that charging can proceed according to enrolled PEV program. [Note: Authentication between Utility and PEV is now complete and charging can proceed according to the enrolled PEV program criteria]

**OECD Security Safeguards Principle:** Utility communicates data through secure interface and confirms data transmission using validation process according to Customer preferences.

Step 17 - PEV prepares for charging based on Customer-selected preferences and enrolled PEV program. Charging may be delayed based upon Customer preferences or grid reliability criteria (e.g., off-peak economy charging, demand response event underway, short, randomized charging delay to promote grid stability, etc.)

**OECD Security Safeguards Principle:** Utility communicates data through secure interface and confirms data transmission using validation process according to Customer preferences.
APPENDIX C: PRIVACY RELATED DEFINITIONS

Because “privacy” and associated terms mean many different things to different audiences, it is important to establish some definitions for the terms used within this chapter to create a common base of understanding for their use. The energy-specific terms are defined within Appendix I. The definitions of the terms related to privacy, as they are used within this chapter, follow.

C.1 PRIVACY IMPACT ASSESSMENT

A privacy impact assessment (PIA) is a structured, repeatable, type of analysis of how information relating to or about individuals, or groups of individuals, is handled. A report, similar to that of an audit report, is generated to describe the types of privacy risks discovered based upon each privacy category, to document the findings, and then to provide recommendations for mitigating the privacy risk findings. Common goals of a PIA include:

1. Determining if the information handling and use within the identified scope complies with legal, regulatory, and policy requirements regarding privacy;
2. Determining the risks and effects of collecting, maintaining, and disseminating information in identifiable, or clear text, form in an electronic information system or groups of systems; and
3. Examining and evaluating the protections and alternative processes for handling information to mitigate the identified potential privacy risks.

C.2 PERSONAL INFORMATION

“Personal information” is a broad term that includes personally identifiable information (PII), in addition to other types of information. Personal information may reveal information about, or describe, an individual, or group of individuals, such as a family, household, or residence. This information includes, but is not limited to, such information as name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, statements made by, or attributed to, the individual, and utility usage information, all of which could be used to impact privacy.

Personal information includes not only PII, as defined below, but also information that may not be specifically covered within existing laws, regulations or industry standards, but does have recognized needs for privacy protections. For example, a social networking site may reveal information about energy usage or creation.

Personal information within the Smart Grid includes, but is not be limited to, information that reveals details, either explicitly or implicitly, about a specific individual’s or specific group’s type of premises and energy use activities. This is expanded beyond the normal "individual" component because there could be negative privacy impacts for all individuals within one dwelling or building structure. This can include items such as energy use patterns, characteristics related to energy consumption through smart appliances, and other types of activities. The energy use pattern could be considered unique to a household or premises similar to how a fingerprint or DNA is unique to an individual.
Personal information also includes energy use patterns that identify specific appliances or devices that may indicate a medical problem of a household member or visitor; the inappropriate use of an employer issued device to an employee that is a household member or visitor; the use of a forbidden appliance in a rented household. Smart appliances and devices will create additional information that may reveal a significant amount of additional personal information about an individual, such as what food they eat, how much they exercise and detailed physical information. This would also become a privacy issue in a university, office setting, healthcare facility and so on.

C.3 PERSONALLY IDENTIFIABLE INFORMATION (PII)

“PII” is information that has been defined within existing laws, regulations and industry standards, as those specific types of information items that can be tied to a unique individual in certain situations and has some current form of legal protection as a result. Such types of information include, but are not necessarily restricted to, the following:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers (including energy bill account numbers, credit card numbers, and so on)
- Certificate and license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device Identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images;
- Any other unique identifying number, characteristic, or code

With the exception of those terms specifically naming energy, the above are the items defined within the Health Insurance Portability and Accountability Act (HIPAA) of 1996,
which arguably has the widest definition of PII within the existing U.S. federal regulations. More identifiers may be added to the list as the Smart Grid evolves and as regulations change.

C.4 COMPOSITE PERSONAL INFORMATION

“Composite personal information” is non-personal information items that, when combined with certain other non-personal information items, can become personal information. In other words, it is the aggregation or combination of non-personal information that reveals insights into personal lives, characteristics and activities, thus forming personal information. Consider a zip code, gender, and birth year. If you look at each of these separately, it would be hard to say you can link each of them to a specific individual. However, if you look at the three items in combination, you may be able to identify a specific individual, particularly in more sparsely populated geographic locations.

C.5 PRIVATE INFORMATION

“Private information” is information that is associated with individuals or groups of individuals, which could reveal details of their lives or other characteristics that could impact them. Private information is not necessarily information that, on its own, is linked to individuals directly.

Private information is typically a classification of information that individuals use for themselves. It is a broad and general term that is more ambiguously used than other privacy terms. For example, the combination to a bank safety deposit lock is private, but the combination number itself does not point to any specific individual. As another example, some individuals consider how they voted in presidential elections to be private information that they do not want any others know. Other individuals, however, communicate how they voted on bumper stickers for the world to see because they have determined that, for them, it is not private information.

Individuals often consider PII to be a type of private information, and personal information could also be private information. For utilities, market data that includes information about a negotiated price for a customer is likely considered by the customer to be private information; they may not want their friends, neighbors or the general public to see this information. Smart device data from within consumer dwellings could also be a type of private information. Private information could cause harm to the associated individuals or groups if misused or accessed by those who do not have a business need. “Private information” is a term used by individuals that indicates information they have determined they do not want others to know, and is not a term used as a data classification type by business organizations.

C.6 CONFIDENTIAL INFORMATION

“Confidential information” is information for which access should be limited to only those with a business need to know, and that could result in compromise to a system, data file, application, or other business function if inappropriately shared. Confidential information is a common term used by businesses as one of their data classification labels. For example, the formula for Coca-Cola is confidential. The plans for a new type of wind turbine, that have not yet been publicized, are confidential.

Market data that does not include customer specific details may be confidential. Many types of personal information can also fall within the “Confidential Information” data classification label. Information can be confidential at one point in the information lifecycle, and then become public.
at another point in the lifecycle. Information that an organization does not want shared outside of their organization, which they consider to be proprietary, is considered to be confidential information. Confidential information must have appropriate safeguards applied to ensure only those with a business need to fulfill their job responsibilities can access the information.

**C.7 INDIVIDUAL**

Any specific person.

**C.8 SMART GRID ENTITY**

An entity that participates within the Smart Grid and that collects, stores, uses, shares, transfers across borders, or retains Smart Grid data.