Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security

The Smart Grid Interoperability Panel
Cyber Security Working Group

September 2010

Table of Contents

1. Introduction and Background

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

At a Glance: Report Objectives

The transformation of today's electricity system into a Smart Grid is both revolutionary and evolutionary. Persistence, diligence, and, most important, sustained public and private partnerships will be required to progress from today's one-way, electromechanical power grid to a far more efficient digitized "system of systems" that is flexible in operations, responsive to consumers, and capable of integrating diverse energy resources and emerging technologies. This progression will unfold over the span of many years, during which several generations of technologies will compose the evolving Smart Grid. As a consequence, the cyber security strategy for the Smart Grid must also be a continuing work in progress so that new or changing requirements are anticipated and addressed.

Guidelines for Smart Grid Cyber Security is both a starting point and a foundation. As Smart Grid technology progresses, the Cyber Security Working Group (CSWG) will continue to provide additional guidance as needed. This first installment of the guidelines is:

- An overview of the cyber security strategy used by the CSWG to develop the high-level cyber security Smart Grid requirements;
- A tool for organizations that are researching, designing, developing, implementing, and integrating Smart Grid technologies—established and emerging;
- An evaluative framework for assessing risks to Smart Grid components and systems during design, implementation, operation, and maintenance; and
- A guide to assist organizations as they craft a Smart Grid cyber security strategy that includes requirements to mitigate risks and privacy issues pertaining to Smart Grid customers and uses of their data.

The guidelines are not prescriptive, nor mandatory. Rather, they are advisory, intended to facilitate each organization's efforts to develop a cyber security strategy effectively focused on prevention, detection, response, and recovery.

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

The three-volume report, NISTIR 7628, *Guidelines for Smart Grid Cyber*

Security[1], presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of Smart Grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information presented in the report as guidance for assessing risk, and then identifying and applying appropriate security requirements to mitigate that risk. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cyber security requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) has *"primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…"*

Effective cyber security is integral to achieving a nationwide Smart Grid, as explicitly recognized in EISA.[2]

> 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.

This initial version of *Guidelines for Smart Grid Cyber Security* was developed as a consensus document by the Cyber Security Working Group (CSWG) of the Smart Grid Interoperability Panel (SGIP), a public-private partnership launched by NIST in January 2010. The CSWG now numbers more than 500 participants from the private sector (including utilities, vendors, manufacturers, and electric service providers), various standards organizations, academia, regulatory organizations, and federal agencies. A number of these members are from outside of the United States.

The *Guidelines* report is a companion document to the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* (NIST Special Publication [SP] 1108),[3] which NIST issued on January 19, 2010. The framework and roadmap report describes a high-level conceptual reference model for the Smart Grid, identifies standards that are applicable (or likely to be applicable) to the ongoing development of an interoperable Smart Grid, and specifies a set of high-priority standards-related gaps and issues. Cyber security is recognized as a critical, cross-cutting issue that must be addressed in all standards developed for Smart Grid applications.

---

[1] NISTIR 7628 is available at http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

[2] Section 1301 of the Energy Independence and Security Act of 2007 (P.L. 110-140).

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

The *Framework* document is the first installment in an ongoing standards and harmonization process. Ultimately, this process will deliver the hundreds of communication protocols, standard interfaces, and other widely accepted and adopted technical specifications necessary to build an advanced, secure electric power grid with two-way communication and control capabilities. Given the transcending importance of cyber security to Smart Grid performance and reliability, the *Guidelines* report "drills down" from the initial release of the *NIST Framework and Roadmap*, providing the technical background and additional details that can inform organizations in their risk management efforts to securely implement Smart Grid technologies. The CSWG will continue to provide additional guidance as the *Framework* document is updated and expanded to address testing and certification, the development of an overall Smart Grid architecture, and as additional standards are identified.

The *Guidelines* document is the product of a participatory public process that, starting in March 2009, included several workshops as well as weekly teleconferences, all of which were open to all interested parties. There were two public reviews of drafts of the report, both announced through notices in the *Federal Register*.[4]

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

Following the executive summary, the first volume of the report describes the approach, including the risk assessment process, used by the CSWG to identify the high-level security requirements. It also presents a high-level architecture followed by a sample logical interface reference model used to identify and define 22 logical interface categories within and across 7 commonly accepted Smart Grid domains. (*See* Figure 2.) High-level security requirements for each of these 22 logical interface categories are then described. The first volume concludes with a discussion of technical cryptographic and key management issues across the scope of Smart Grid systems and devices.

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

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

Another recommendation is to educate consumers and other individuals about the potential privacy risks within the Smart Grid and what they can do to mitigate these risks.

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

For all sections except the Executive Summary and Volume 2, it is assumed that readers of the report have a functional knowledge of the electric power grid and a functional understanding of cyber security.

2. Cyber Security Context: Today's Grid, Tomorrow's Smart Grid

Sometimes called the world's largest interconnected machine, the electric power system is the most capital-intensive infrastructure in North America.[5] The system is undergoing tremendous change that will unfold over a number of years. As the grid is modernized, it will become highly automated, leverage information technology more fully, and become more capable in managing energy from a variety of distributed sources. However, in this process of becoming increasingly "smarter," the grid will expand to contain more interconnections that may become portals for intrusions, error-caused disruptions, malicious attacks, and other threats.

The *Cyberspace Policy Review* initiated by President Obama advised that "the Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources." Specifically, the review recommended that as "the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks."[6]

Given that over 80 percent of the physical assets that make up the grid (generating plants, transmission and distribution lines, meters, and more) are privately owned, coordination and collaboration between the public and private sectors is essential to securing this vital infrastructure and ensuring safe and reliable delivery of high-quality electricity.

---

[5] Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, *Critical National Infrastructures*, April 2008.

[6] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009. Available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

In the 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, as well as 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. To a significant degree, coordination has been accomplished by linking systems with embedded, stand-alone communication networks. In fact, in today's grid, much communication and coordination continues to be accomplished by means of the telephone.

However, effective recording, processing, and exchanging of data is becoming increasingly critical to the reliability of the power system. For example, in the August 14, 2003, blackout, a contributing factor was issues with delays in communications alert responses 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 due not to any terrorist or Internet hacker attack; the failures were caused by inadvertent events—mistakes, lack of key alarms, and poor design.

As illustrated by the 2003 blackout, cyber security must address not only deliberate attacks, 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.

Clearly, the convergence of the information and communication infrastructure with the electric power grid introduces new security and privacy-related challenges. However, the introduction of these technologies to the electric sector also presents opportunities to increase the reliability of the power system, to make it more capable and more resilient to withstand attacks, equipment failures, human errors, natural disasters, and other threats. Greatly improved monitoring and control capabilities must include cyber security solutions in the development process rather than as a retrofit.

A few examples of potential risks associated with the evolution of the Smart Grid include:

- Greater complexity increases exposure to potential attackers and unintentional errors;
- Networks that link more frequently to other networks introduce common vulnerabilities that may now span multiple Smart Grid domains (see Figure 2) and increase the potential for cascading failures;
- More interconnections present increased opportunities for "denial of service" attacks, introduction of malicious code (in software/firmware) or compromised hardware, and related types of attacks and intrusions;
- As the number of network nodes increases, the number of entry points and paths that potential adversaries might exploit also increases; and
- Extensive data gathering and two-way information flows may broaden the potential for compromises of data confidentiality and breaches of customer privacy, and compromises of personal data and intrusions of customer privacy.

Components of Cyber Security Strategy*

Prevention: Actions taken and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervene and stop an occurrence, or to mitigate effects.

Detection: Approaches to identify anomalous behaviors and discover intrusions, detect malicious code, and other activities or events that can disrupt electric power grid operations, as well as techniques for digital evidence gathering.

Response: Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes.

Recovery. Development, coordination, and execution of service- and site-restoration plans for affected facilities and services; reconstitution of Smart Grid operations and services through individual, private-sector, nongovernmental, and public–sector actions.

*Adapted from: U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 2009. Available at: http://www.dhs.gov/files/programs/editorial_0827.shtm#0.

The *Guidelines* document describes an approach for assessing cyber security issues and selecting and modifying cyber security requirements to address these issues. It is designed to facilitate identification of requirements that are specific to individual or multiple domains of the Smart Grid. A key aim of the report is to ensure the interoperability of security solutions across the infrastructure. For each stakeholder, every domain, and the entire Smart Grid, the goal is to develop a cyber security strategy that effectively addresses prevention, detection, response, and recovery. The *Guidelines* are not meant to be prescriptive or definite, but rather a flexible framework to be applied to securing the Smart Grid from an operational and technology development perspective.

3. CSWG's Methodology for Developing the Guidelines

Development of an effective cyber security strategy requires a holistic approach to analyzing risk. For example, an effective risk assessment approach entails "*systematically documenting and prioritizing known and suspected control system vulnerabilities [threats] and their potential consequences,"* so that *"energy sector asset owners and operators will be better prepared to anticipate and respond to existing and future threats."*[7]

Risk is the potential for an unwanted outcome resulting from internal or external factors, as determined from the likelihood of occurrence and the associated consequences. Organizational risk can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk, and the risk from information systems). As

[7] U.S. Department of Energy, U.S. Department of Homeland Security, *Roadmap to Secure Control Systems in the Energy Sector,* January 2006. Available at: http://www.oe.energy.gov/csroadmap.htm.

shown in the generic model in Figure 1, risk is the product of interactions among threats, vulnerabilities, and consequences.

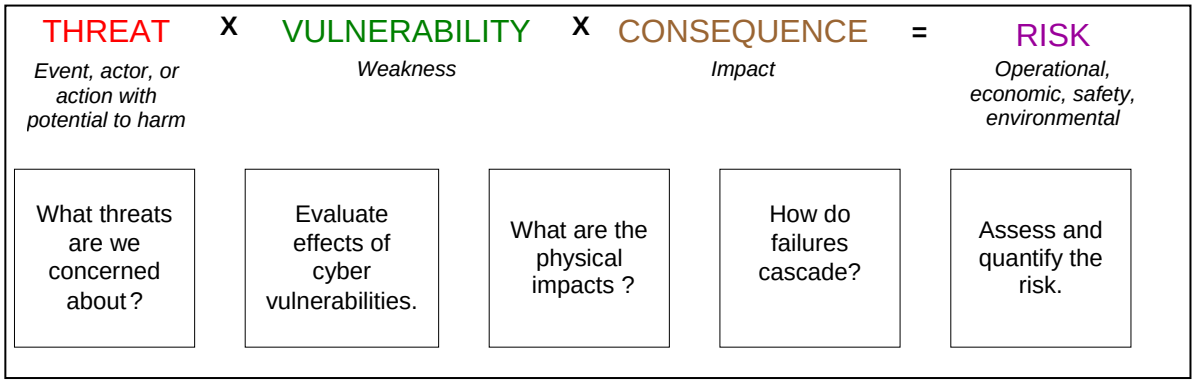

Figure 1. Generic model of risk

The Smart Grid risk assessment process is based on existing risk assessment approaches developed by both the private and public sectors. It includes identifying assets, vulnerabilities, and threats and specifying potential 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 power system technology domains, the risk assessment process is applied to all three domains as they interact in the Smart Grid.

The CSWG used a five-step methodology for developing the *Guidelines* document, as outlined below.

3.1 Step 1: Selection of Use Cases with Cyber Security Considerations

The first step was the identification of Smart Grid use cases,[8] which document system interactions and behaviors that occur—or could occur—during Smart Grid application scenarios. It was a necessary preliminary step, providing the input for assessing risk. An example of a use case scenario is remotely reading an electric meter. Volume 3, Chapter 10 of the *Guidelines* details a set of use cases considered to be especially salient to the task of determining Smart Grid security requirements. The use case set provided a common framework for performing the risk assessment, developing the logical reference model, and selecting and tailoring the high-level security requirements.

3.2 Step 2: Performance of a Risk Assessment

The second step was conducting the risk assessment on the use cases. Each use case was reviewed from a high-level, overall functional perspective that included identifying assets, vulnerabilities, and threats and the specification of potential impacts. The output was used as the

[8] Use cases capture who (actors) does what (interactions) with the system, for what purpose (goal). A complete set of use cases specifies all the different ways to use the system, and thus defines all behavior required of the system--without dealing with the internal structure of the system. (Excerpted from *Functional Requirements and Use Cases* [2001], by Ruth Malan and Dana Bredemeyer. Download from: http://www.bredemeyer.com/pdf_files/functreq.pdf.

baseline for the selection of security requirements and the identification of gaps in guidance and standards related to the security requirements.

The risk assessment focuses on Smart Grid operations and not on systems used to run business operations. However, organizations should capitalize on existing enterprise infrastructures, technologies, support, and operational aspects when designing, developing, and deploying Smart Grid information systems.

Both bottom-up and top-down approaches were used in performing the risk assessment. The bottom-up approach focused 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. In the top-down approach, logical interface diagrams were developed for the six functional priority areas that were the focus in the initial draft of the *Guidelines* document—Electric Transportation, Electric Storage, Wide Area Situational Awareness, Demand Response, Advanced Metering Infrastructure, and Distribution Grid Management. These logical interface diagrams, found in Volume 3, Appendix F of the report, were instrumental in the later task of constructing a logical reference model.

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 assessment outcome. The Smart Grid is no different. The report recommends that all organizations take a realistic view of the hazards and threats, and work with national authorities as needed to acquire the required information.

3.3 Step 3: Setting Boundaries: The Beginnings of a Security Architecture

The third step required the development of security 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. Across the seven domains, numerous actors will capture, transmit, store, edit, and process the information necessary for Smart Grid applications.

In general, actors in the same domain have similar objectives. To enable Smart Grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 2. However, communications within the same domain may not necessarily have similar characteristics and requirements. For example, for communications or information within the Customer domain, simple meter reads have simple characteristics and requirements such as a meter communicates with a specific utility head-end system, while a customer portal needs to have multiple users accessing it at the same time to different accounts. Moreover, particular domains may contain components of other domains. For instance, the ten Independent System Operators and Regional Transmission Organizations (ISOs/RTOs) in North America have actors in both the Markets and Operations domains. Similarly, a distribution utility is not entirely contained within the Distribution domain—it is likely to contain actors in the Operations domain, such as a distribution management system, and in the Customer domain, such as meters.

As explained more fully in Chapter 2, the document presents a composite view of 46 *actors* distributed among the 7 domains, as shown in Figure 3. The actors do not comprise all the devices, computer systems, software programs, individuals, and organizations participating in the Smart Grid. Rather, they serve as a representative set of actors for the purpose of the analysis begun by the CSWG. A full list of the sample actors, complete with descriptions, may be found in Volume 1, Table 2-1.

One output of this analysis is a logical reference model that shows logical interfaces linking actors and suggests the types of information exchanged. The purpose of the logical reference model is to break down the Smart Grid and the domains into more granular detail, but not defining interface specifications and data types. This model focuses on a short-term view (one to three years) of the proposed Smart Grid and is only a sample representation. It can serve as a vehicle for identifying, organizing, prioritizing, and communicating security requirements and the security-related responsibilities of actors.

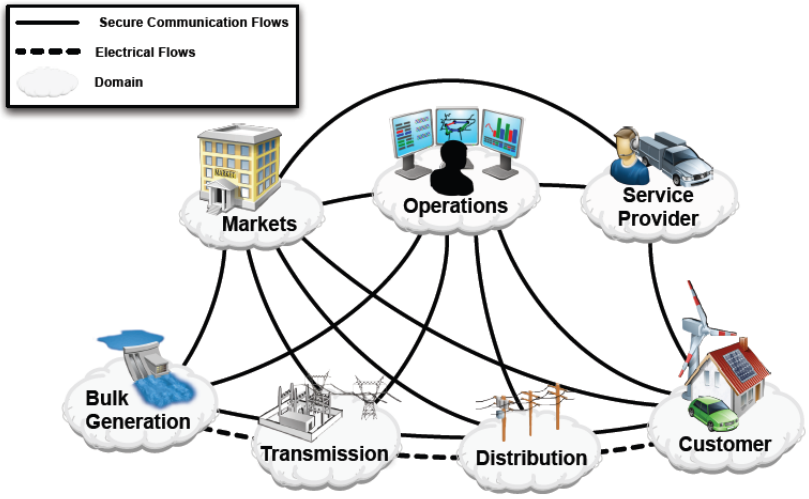

Figure 2. Interaction among actors in Smart Grid domains through secure communication flows and flows of electricity.

Source: *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108)*

Over 130 possible logical interfaces were identified. These interfaces (shown in Figure 3) were assigned to one of 22 categories on the basis of shared or similar security characteristics. For instance, category 13 covers the logical interfaces between systems that use the Advanced Metering Infrastructure (AMI) network. Having these categories simplifies the identification of security *requirements* for each interface.

For each of the 22 categories of Smart Grid interfaces, the CSWG evaluated the impact of an equipment failure, intrusion, and other security threats on the three security objectives of Smart Grid performance, information, and information systems. Rated as low, moderate, or high, impact levels were assigned for—

- Loss of ***confidentiality***—the unauthorized disclosure of information;
- Loss of ***integrity***—the unauthorized modification or destruction of information; and
- Loss of ***availability***—the disruption of access to or use of information or an information system.

Even at the high-level perspective of the logical reference model, it should be clear that security must be applied in layers, with one or more security measures and controls implemented at each layer. The objective is to mitigate the risk so that if one component of the defense is compromised or circumvented, the result will not be a cascading set of failures. Because no

single security measure can counter all types of threats, multiple levels of security measures should be implemented.

This layered approach to security should leverage existing power system design and capabilities that have been successful in assuring reliable supplies of power to consumers. Existing power system defenses and safeguards that protect against—or mitigate—outages due to inadvertent actions and natural disasters may be used to address some of the cyber security requirements.

The logical reference model does not imply any specific implementation. The model is a work in progress, and it will be revised and undergo further development. Additional underlying detail, as well as additional Smart Grid functions, will be needed to enable more detailed analysis of required security functions. This work will complement and draw on the contributions of the SGIP's Smart Grid Architecture Committee (SGAC).

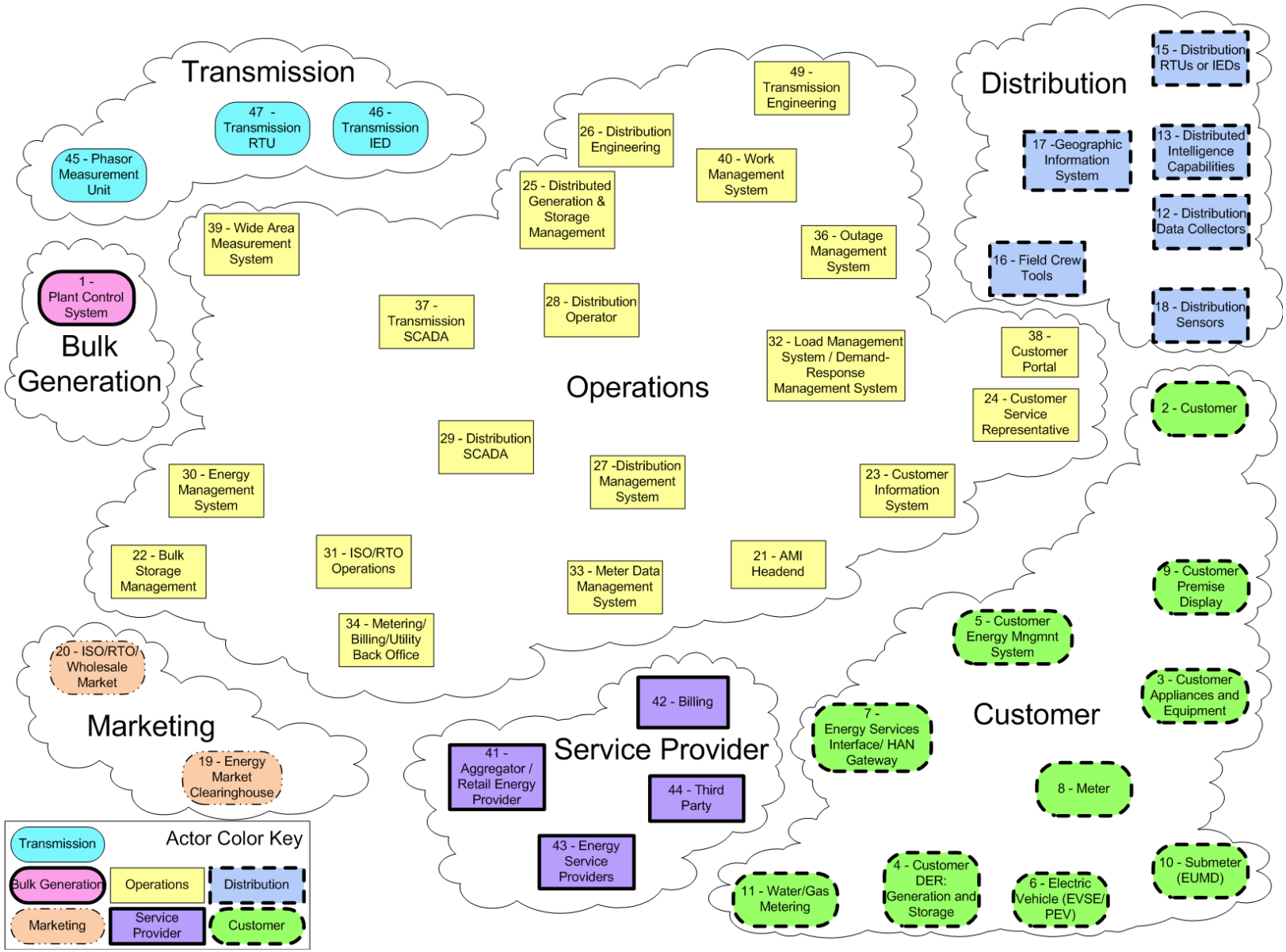

Figure 3 - Composite High-Level View of the Actors within Each of the Smart Grid Domains

3.4 Step 4: High-Level Security Requirements

The fourth step in developing the *Guidelines* document was to describe over 180 high-level security requirements selected by the CSWG as applicable to the entire Smart Grid or to particular domains and interface categories. The requirements were chosen from a large collection of requirements reviewed by the CSWG.[9] This initial set of high-level security requirements is not definitive, nor is it intended to be prescriptive. These requirements are sorted into 19 groups, or "families, with similar objectives." Examples of these families are Access Control, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, and Personnel Security.

Organizations may use the CSWG's set of high-level requirements as a baseline as they devise their cyber security strategies. The approach to securing the Smart Grid is described in the *Guidelines* document by performing the following:

- ***Determine the logical interface categories.*** A thorough analysis of the actors, domains, information systems, and network and communications requirements is necessary to adequately determine the logical interface categories.
- ***Assess risk.*** Identify the threats, security constraints, and issues associated with each logical interface category along with the impact (low, moderate, or high) to the organization if there is a compromise of confidentiality, integrity, and/or availability.
- ***Select the initial set of baseline security requirements based on the logical interface categories.*** Tailor and supplement the security requirements as needed based on an organizational assessment of risk and local conditions.

Additional criteria should be used in determining the cyber security requirements before selecting and implementing specific measures or solutions such as the characteristics of the interface, including the information, constraints, and issues posed by device and network technologies, the existence of legacy systems and devices, varying organizational structures, regulatory and legal policies, and cost criteria.

It is important to note that the requirements related to emergency lighting, fire protection, temperature and humidity controls, water damage, power equipment and power cabling, and lockout/tagout[10] are important requirements for safety. However, these are outside the scope of cyber security and are not included in this report. These requirements must be addressed by each organization in accordance with local, state, federal, and organizational rules, policies, and procedures.

Each of the high-level security requirements was assigned to one of three categories indicating where within an organization, operation, or function a particular requirement should be implemented. These are:

[9] NIST Special Publication 800-53 *Recommended Security Controls for Federal Information Systems*; DHS *Catalog of Control Systems Security: Recommendations for Standards Developers*, and NERC CIPS (1-9).

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

- ***Governance, risk, and compliance (GRC) requirements:*** Addressed at the organizational level and relevant to all Smart Grid organizations, but it may be necessary to augment these organization-level requirements for specific logical interface categories and/or Smart Grid information systems;
- ***Common technical requirements:*** Applicable to all of the 22 logical interface categories; and
- ***Unique technical requirements:*** Applicable to one or more—but not all—of the 22 interface categories.

The common and unique technical requirements should be allocated to each Smart Grid system and not necessarily to every component within a system, as the focus is on security at the system level and not on specific information exchanges between components. Each organization must develop a security architecture for each Smart Grid information system and allocate security requirements to components/devices. Some security requirements may be allocated to one or more components/devices. However, not every security requirement must be allocated to every component/device. Impact levels for a specific Smart Grid information system—and, therefore, the need to implement enhancements to specific requirements— will be determined by organizations during the risk assessment process.

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

Table 3-3 in the *Guidelines* document shows all of the selected requirements and the baseline impact level (low, moderate, or high) for each of the 22 interface categories.

3.4.1 Information Included with Each Security Requirement

Each of the requirements is presented in a standard format with the following information—

Security requirement identifier and name. Each security requirement has a unique identifier that consists of three components. The initial component is SG – for Smart Grid. The second component is the family name, e.g., AC for Access Control and CP for Continuity of Operations. The third component is a unique numeric identifier, for example, SG.AC-1 and SG.CP-3. Each requirement also has a unique name.

Category. The category identifies whether the security requirement is a GRC, common technical requirement, or unique technical requirement. For each common technical security requirement, the most applicable objective (confidentiality, integrity, and availability) is listed.

The *Requirement* describes specific security-related activities or actions to be carried out by the organization or by the Smart Grid information system.

The *Supplemental Guidance* section provides additional information that may be useful in understanding the security requirement. This information is guidance and is not part of the security requirement.

The *Requirement Enhancements* provide statements of security capability to (i) build additional functionality in a requirement, and/or (ii) increase the strength of a requirement. In both cases, the requirement enhancements are used in a Smart Grid information system requiring greater protection due to the potential impact of loss based on the results of a risk assessment. Requirement enhancements are numbered sequentially within each requirement.

The *Additional Considerations* provide additional statements of security capability that may be used to enhance the associated security requirement. These are provided for organizations to consider as they implement Smart Grid information systems and are not intended as security requirements. Each additional consideration is number A1, A2, etc., to distinguish them from the security requirements and requirement enhancements.

The *Impact Level Allocation* identifies the security requirement and requirement enhancements, as applicable, at each impact level: low, moderate, and high. The impact levels for a specific Smart Grid information system will be determined by the organization in the risk assessment process.

3.4.2 A Walk-Through Example of Choosing Security Requirements

Smart Grid control system "ABC" includes an interconnection between a plant control system and an energy management system. As specified in Volume 1, Table 3-2, this interconnection is identified as logical interface category 6 and requires high data accuracy, moderate availability, and only low confidentiality protections.

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

Next the organization will need to review Table 3-3 in order to determine which of the common and unique technical requirements are applicable to logical interface category 6. They will then need to determine if any of these requirements need to be modified or augmented for the ABC control system, just as they did with the GRC requirements.

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

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

3.5 Step 5: Smart Grid Conformity Testing and Certification

In order to support interoperability of Smart Grid systems and products, Smart Grid products developed to conform to those interoperability standards should undergo a rigorous conformity and interoperability testing process. NIST has initiated a program to develop a Smart Grid Conformity Testing Framework that will be further refined and maintained by the Smart Grid Interoperability Panel. Within NIST's three-phase plan to expedite the acceleration of interoperable Smart Grid standards, Smart Grid conformity testing is designated as Phase III. Smart Grid conformity testing has been included in the work of the SGIP in recognition of the importance of Smart Grid conformity testing and the need to couple to standards identified for the Smart Grid. This includes establishing a permanent Testing and Certification Committee within the SGIP.

In today's standards environment, it is important to eliminate duplication of work activities related to Smart Grid standards as well as conformity testing. Recognizing that some efforts exist today to test certain Smart Grid standards and others are under way, NIST's intention is to leverage existing programs wherever practical. Hence the first step in developing a Smart Grid Conformity Testing Framework is to perform an analysis of existing SG standards conformity testing programs. An in-depth study has been initiated to identify and describe existing conformity assessment programs for Smart Grid products and services based on standards and specifications identified in the NIST *Framework and Roadmap* document. This survey will address, in particular, conformity assessment programs assuring interoperability, cyber security, and other relevant characteristics. Descriptions of these programs will include all elements of a conformity assessment system, including accreditation bodies, certification bodies, testing and calibration laboratories, inspection bodies, personnel certification programs, and quality registrars. The study will also identify present gaps and deficiencies in these existing conformity assessment programs.

In addition, a report outlining the conformity assessment requirements of federal and state governments and other relevant SG stakeholders will be developed.

The results of this study will provide an input to the SGIP's Testing and Certification Committee. The SGIP Testing and Certification Committee will have continuing visibility of Smart Grid conformity testing and certification existing in the industry; recommend improvements and means to fill gaps; and work with current standards bodies and user groups to develop new test programs to fill voids.

Feedback from Standard Developing Organizations and other relevant bodies is another important aspect of the Smart Grid Conformity Testing Framework. Errors, clarifications, and enhancements are typically identified to existing standards throughout the normal conformity testing process. In order to improve interoperability, an overall process is critical to ensure that changes and enhancements are incorporated continuously.

4. Beyond the Security Requirements: Other Parts of the Report

The final step in completing the *Guidelines* document was to share the results of the Research and Development subgroup and the Privacy subgroup.

4.1 Research and Development Themes for Smart Grid Cyber Security

Current state-of-the-art security technology needs to be improved in order to realize the envisioned functional, reliability, and scalability requirements necessary to build a secure, fully integrated Smart Grid. While deployment of today's advanced hardware and software has placed many parts of the power system on the modernization path, sustained progress in research and

development (R&D) is necessary to upgrade legacy systems that were fielded with limited automation and that have limited flexibility.

The CSWG has identified an initial set of high-priority R&D challenges arranged into the following categories:

- ***Device level***, where research can guide efforts to devise cost-effective, tamper-resistant architectures for smart meters and other components, which are necessary for systems-level survivability and resiliency and for improving intrusion detection in embedded systems.
- ***Cryptography and key management***, to enable key management on a scale involving, potentially, tens of millions of credentials and keys as well as local cryptographic processing on the sensors such as encryption and digital signatures.
- ***Systems level,*** where research on a number of related topics is required to further approaches to building advanced protection architecture that can evolve and can tolerate failures, perhaps of a significant subset of constituents.
- ***Networking issues,*** which include research to investigate ways to ensure that commercially available components, public networks like the Internet, or available enterprise systems can be implemented without jeopardizing security or reliability.

In addition to topics discussed in the R&D chapter, the CSWG identified a diverse range of other cyber security-related topics—from privacy and access control to denial-of-service resiliency to improved models and tools for identifying vulnerabilities and detecting anomalous behavior—that can significantly improve the effectiveness of measures to safeguard the Smart Grid.

4.2 Privacy and the Smart Grid

The CSWG Privacy subgroup views the privacy chapter (Volume 2) as a starting point for continuing the work to improve upon privacy practices as the Smart Grid continues to evolve and as new privacy threats, vulnerabilities, and the associated risks emerge. The information in this chapter was developed as a consensus document by a diverse subgroup consisting of representatives from the privacy, electric energy, telecommunications and cyber industries, academia, and government organizations. The chapter does not represent legal opinions, but rather was developed to explore privacy concerns and provide associated recommendations for addressing them. Privacy impacts and implications may change as the Smart Grid expands and matures.

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. Four dimensions of privacy are considered: (1) personal information—any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural, locational, or social identity; (2) personal privacy—the right to control the integrity of one's own body; (3) behavioral privacy—the right of individuals to make their own choices about what they do and to keep certain personal behaviors from being shared with others; and (4) personal communications privacy—the right to communicate without undue surveillance, monitoring, or censorship.

Most Smart Grid entities directly address the first dimension, because privacy of personal information is what most data protection laws and regulations cover. However, the other three

dimensions are important privacy considerations as well and should be considered by Smart Grid entities.

When considering how existing laws may deal with privacy issues within the Smart Grid, and likewise the potential influence of other laws that explicitly apply to the Smart Grid, it is important to note that while Smart Grid privacy concerns may not be expressly addressed, existing laws and regulations may still be applicable. Nevertheless, the innovative technologies of the Smart Grid pose potential new issues for protecting consumers' privacy that will have to be tackled by law or other means.

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

The research behind the material presented in this chapter focused on privacy within personal dwellings and electric vehicles, and did not address business premises and the privacy of individuals within such premises.

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

- Conduct pre-installation processes and activities for using Smart Grid technologies with utmost transparency.
- Conduct an initial privacy impact assessment before making the decision to deploy and/or participate in the Smart Grid. Additional privacy impact assessments should be conducted following significant organizational, systems, applications, or legal changes—and particularly, following privacy breaches and information security incidents involving personal information, as an alternative, or in addition, to an independent audit.
- Develop and document privacy policies and practices that are drawn from the full set of Organization for Economic Cooperation and Development (OECD) Privacy Principles and other authorities (*see* Volume 2, Chapter 5, Section 5.4.1 "Consumer-to-Utility PIA Basis and Methodology"). This should include appointing personnel responsible for ensuring that privacy policies and protections are implemented.
- Provide regular privacy training and ongoing awareness communications and activities to all workers who have access to personal information within the Smart Grid.
- Develop privacy use cases that track data flows containing personal information to address and mitigate common privacy risks that exist for business processes within the Smart Grid.
- Educate consumers and other individuals about the privacy risks within the Smart Grid and what they can do to mitigate them.

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

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

5. Conclusion

As the United States continues to transform the electric power infrastructure, new risks and threats will evolve. The electric power industry needs to remain vigilant to ensure energy efficiency, reliability, and security; to transition to renewable sources of energy; to reduce greenhouse gas emissions; and to build a sustainable economy that ensures future prosperity. The three-volume report, *Guidelines for Smart Grid Cyber Security*, presents an actionable initial analytical framework that organizations can use to develop effective cyber security strategies and solutions tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities.