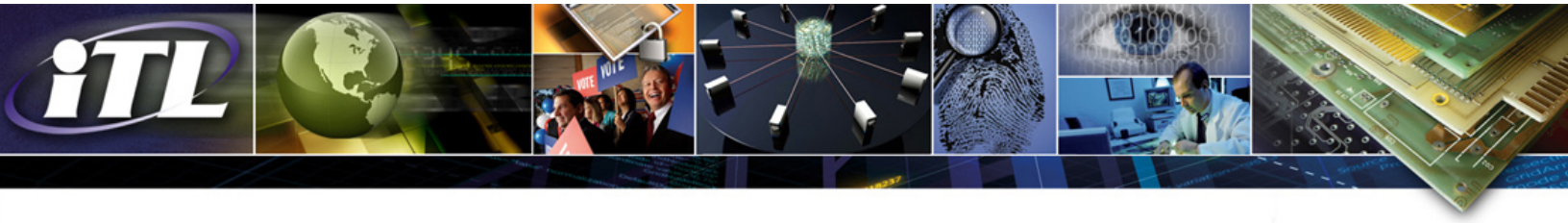


ITL BULLETIN FOR SEPTEMBER 2014

RELEASE OF NIST INTERAGENCY REPORT 7628 REVISION 1, GUIDELINES FOR SMART GRID CYBERSECURITY

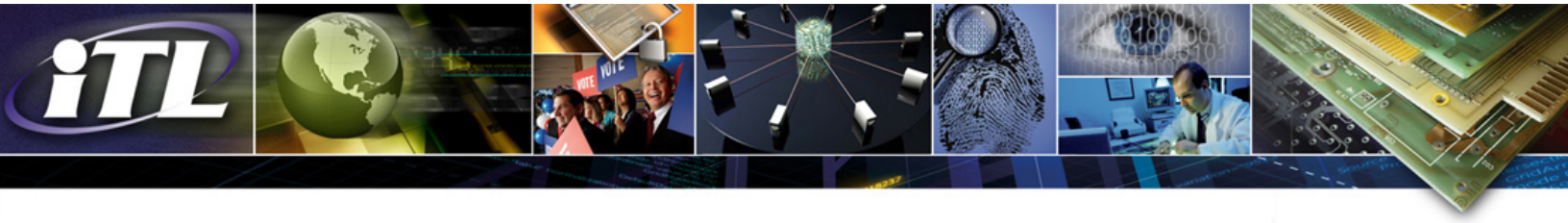
Victoria Yan Pillitteri, Tanya Brewer, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

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—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.

Smart grid technology and implementations have evolved significantly since NIST first published NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security,* in 2010. Since then, the community has generally moved from a notional vision to actual deployments. Feedback on the report and users' experience deploying smart grid systems provided an opportunity to revisit and update the architecture, interfaces, and actors. Additionally, new sections were included to address outstanding issues from the original publications, such as cyber-physical attacks. The regulatory requirements regarding privacy and the smart grid have also changed considerably since 2010, as well as the understanding of how certain pieces of smart grid technology function in real-world deployments. This necessitated some updates regarding privacy in the smart grid.

This three-volume report, NISTIR 7628 Rev. 1, *Guidelines for Smart Grid Cybersecurity*, presents a voluntary framework that can be used by organizations to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of smart grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information presented in this report as guidance for assessing risk and identifying and applying appropriate security requirements. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment with expanded roles of the information technology (IT) and telecommunications infrastructures. Therefore, the cybersecurity of systems and information in the IT and telecommunications infrastructures must be addressed by an evolving electric sector. Cybersecurity must be included in all phases of the system development life cycle, from design phase through implementation, maintenance, and disposition. The information included in this document is guidance for organizations. NIST does not prescribe particular solutions



through the guidance contained in this document. Each organization will develop its own detailed cybersecurity approach (including a risk assessment methodology) for the smart grid.

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

Document Development Strategy

NISTIR 7628 Rev. 1 provides background information on the smart grid and the importance of cybersecurity in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the cybersecurity strategy for the smart grid and the following specific tasks within this strategy:

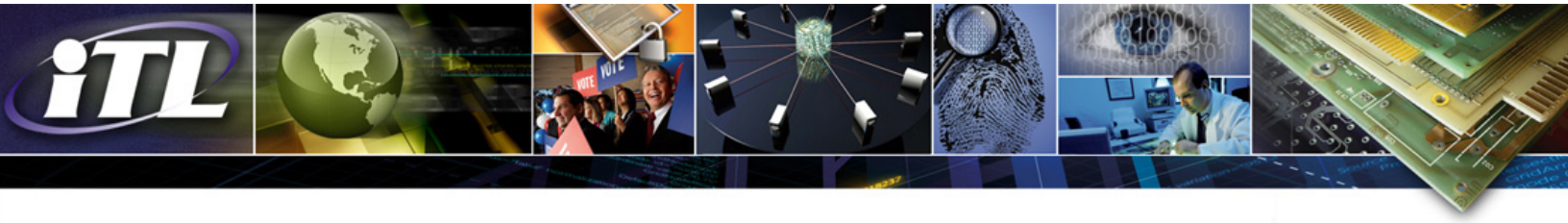
Task 1. Selection of use cases with cybersecurity considerations;
Task 2. Performance of a risk assessment;
Task 3. Specification of high-level security requirements;
Task 4a. Development of a logical reference model;
Task 4b. Assessment of Smart Grid standards; and
Task 5. Conformity Assessment.

NISTIR 7628 Rev. 1 addresses cybersecurity using the tasks described above, resulting in a general set of requirements. These requirements are developed (or augmented, where standards/guidelines already exist) using a high-level risk assessment process that is defined in the cybersecurity strategy. The overall strategy used in the development of this document examined both domain-specific and common requirements when developing a risk mitigation approach to ensure interoperability of solutions across different parts of the infrastructure.

The document development strategy required the definition and implementation of an overall cybersecurity risk assessment process for the smart grid. *Risk* is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. This type of risk is one component of organizational risk, which can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk, the risk from information systems). The smart grid risk assessment process is based on existing risk assessment approaches developed by both the private and public sectors, and includes identifying assets, vulnerabilities, and threats and specifying impacts to produce an assessment of risk to the smart grid and to its domains and subdomains, such as homes and businesses. Because the smart grid includes systems from the IT, telecommunications, and electric sectors, the risk assessment process is applied to all three sectors as they interact in the smart grid.

Logical Architecture and Interfaces of the Smart Grid

The high-level security requirements (found in Chapter 3) describe *what* the smart grid needs to deliver to enhance security. The logical security architecture (found in Chapter 2) describes *where*, at a high level, the smart grid needs to provide security. Chapter 2, *Logical Architecture and Interfaces of the Smart Grid*, provides a high-level diagram that depicts a composite high-level view of the actors within each of the smart grid domains. 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. This overall logical reference model of the smart grid includes the seven domains within the smart grid: Transmission, Distribution, Operations, Generation, Markets, Customer, and Service Provider. The various actors (e.g., devices, systems, or programs) are needed to transmit, store, edit, and process the information needed within the smart grid.

The logical reference model represents a blending of the initial set of use cases, requirements that were developed at the NIST smart grid workshops in 2009, the initial NIST Smart Grid Interoperability Roadmap, and the logical interface diagrams for the six Federal Energy Regulatory Commission (FERC) and NIST priority areas: electric transportation, electric storage, advanced metering infrastructure (AMI), wide-area situational awareness (WASA), distribution grid management, and customer premises. While the original diagrams for these six areas were included in the original version of the document, they have been removed from the Revision to avoid confusion since the logical reference model has evolved in a number of ways since 2010.

Each logical interface—the connection between two actors—in the logical reference model was allocated to a logical interface category. This was done because many of the individual logical interfaces are similar in their security-related characteristics and can, therefore, be categorized together as a means to simplify the identification of the appropriate security requirements. These security-related logical interface categories (LICs) were defined based on attributes that could affect the security requirements. NISTIR 7628 Rev. 1 includes descriptions and individual diagrams showing the relevant actors and interfaces for each of the 22 LICs. Since the first publication of the document, real-world implementations of smart grid technology have progressed across the country. With this progression has come a better understanding of how different components of the smart grid interface, or do not interface, with each other. The logical reference model has been updated to reflect real-world implementations as much as possible.

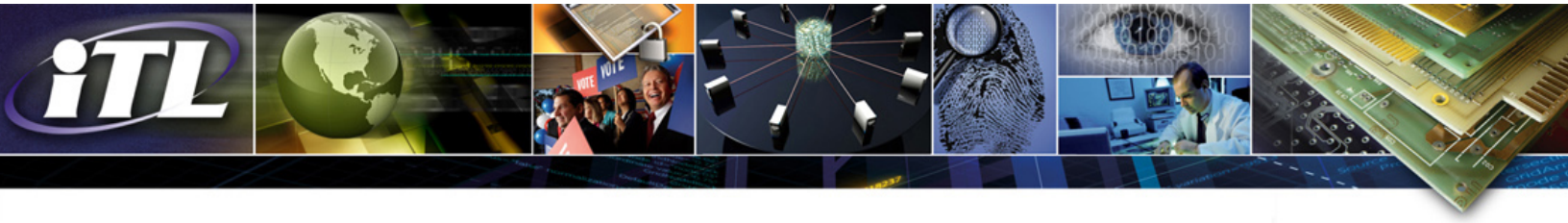
NISTIR 7628 Rev. 1 also provides an overview of a defense-in-depth approach in Chapter 2.

High-Level Security Requirements

Chapter 3, *High-Level Security Requirements*, specifies the high-level security requirements for the smart grid for each of the 22 LICs. It provides guidance and a starting point for selecting and modifying security requirements to organizations that are implementing, designing, and/or operating smart grid systems. To supplement the guidance in this chapter, each organization should perform a risk assessment to determine the applicability of the material in this chapter. No significant changes to the high-level security requirements were made as part of the revision.

Chapter 3 includes the detailed descriptions for each of the recommended security requirements that have been tailored for smart grid information systems, and includes the following additional elements:

- Determination of the confidentiality, integrity, and availability impact levels for each of the logical interface categories;
- The recommended security requirements allocated to the 22 LICs originally discussed in Chapter 2;
- Additional background and guidance on the selection of security requirements; and
- A new section on Testing and Certification of Smart Grid Cybersecurity.



Cryptography and Key Management

Chapter 4 identifies technical cryptographic and key management issues across the scope of systems and devices found in the smart grid along with potential alternatives. The identified alternatives may be existing standards, methods, or technologies, and their optimal adaptations for the smart grid. Where alternatives do not exist, the gaps have been identified where new standards and/or technologies should be developed for the industry. This chapter has been updated to reference the recommended transition lifetimes for cryptographic algorithms and key lengths in NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*.

Privacy and the Smart Grid (Volume 2)

NISTIR 7628 Rev. 1 includes an initial discussion about what privacy is, a summary of a privacy impact assessment (PIA) for the smart grid conducted in 2009, potential privacy issues with regards to the smart grid, and a discussion of mitigation strategies for these potential issues. The report also provides an overview of some existing privacy risk mitigation regulations and frameworks. It includes privacy use cases developed using the overall smart grid use cases found later in Volume 3. Each use case is provided with case-specific data privacy recommendations. In particular, Volume 2 considers potential future privacy issues related to new applications, such as social media and Plug-In Electric Vehicles (PEVs). Finally, Chapter 5 includes a set of recommendations to help mitigate the privacy issues discussed during the rest of the volume. Supporting material in the appendices goes into more depth for topics such as regulatory changes in California and Colorado, the PIA from 2009, recommendations for how third parties should handle customers' energy usage data, and the full set of use cases.

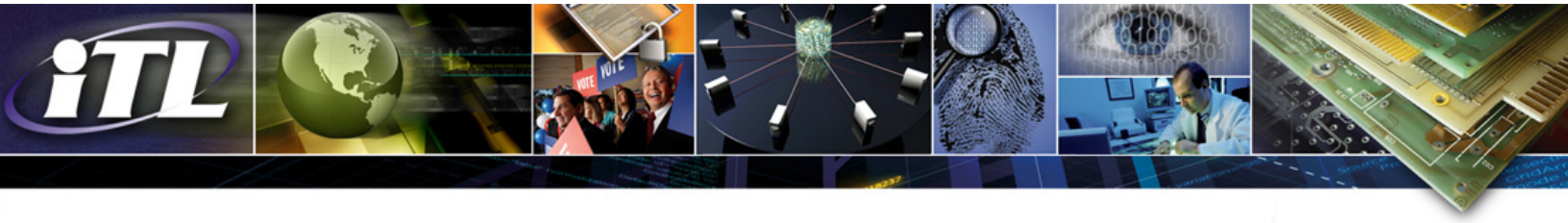
Supportive Analyses and References (Volume 3)

Vulnerability Classes

Chapter 6 is intended for use by those responsible for designing, implementing, operating, or procuring any part of the electric grid. This section contains a list of four classes of potential vulnerabilities with descriptions of specific areas that can make an organization vulnerable as well as the possible impacts to an organization should the vulnerability be exploited. For the purpose of this document, a vulnerability class is a category of weakness which could adversely impact the operation of the electric grid. A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Bottom-Up Security Analysis

Chapter 7 identifies specific protocols, interfaces, applications, and best practices that could and should be developed to solve specific smart grid cybersecurity problems. The section identifies some specific problems and issues that need to be addressed, but does not perform a comprehensive gap analysis that covers all possible cybersecurity issues.



Research and Development Themes for Cybersecurity in the Smart Grid

Cybersecurity is one of the key technical areas where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the smart grid. Chapter 8 is the deliverable originally produced by the R&D subgroup of Smart Grid Interoperability Panel-CyberSecurity Working Group (SGIP-CSWG) based on the inputs from various group members with updates made for the first revision of this document. In general, this chapter distills research and development themes that are meant to present paradigm-changing directions in cybersecurity that will enable higher levels of reliability and security for the smart grid as it continues to become more technologically advanced.

Overview of the Standards Review

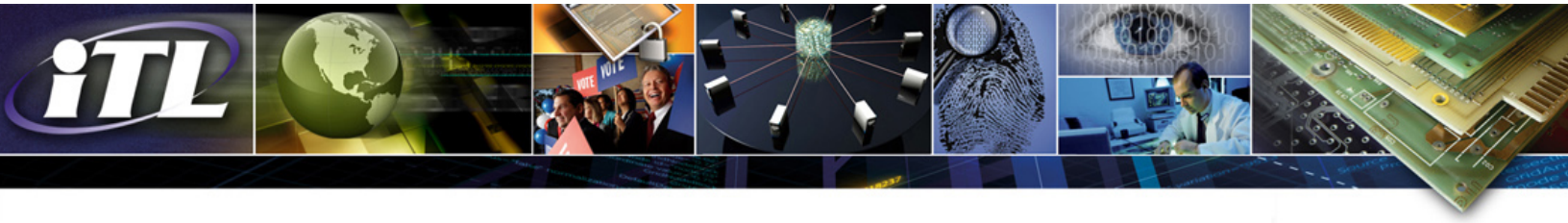
The objective of the standards review discussed in Chapter 9 is to ensure that identified standards applicable to the smart grid adequately address the cybersecurity requirements included in this document. If the standards do not have adequate coverage, relative to their intended scope, this review will identify where changes may need to be made or where other standards may need to be applied to provide sufficient coverage in that area. This standards review is part of the process to include a standard into the SGIP Catalog of Standards. This chapter has been updated to reflect the Smart Grid Interoperability Panel Cybersecurity Committee review and analysis methodology of identified standards against the high-level security requirements of NISTIR 7628.

Key Power System Use Cases for Security Requirements

The focus of Chapter 10 is to identify the key use cases that are architecturally significant with respect to security requirements for the smart grid. This identification is neither exhaustive nor complete. The use cases presented in this chapter will be employed in evaluating smart grid characteristics and associated cybersecurity objectives; the high-level requirements of confidentiality, integrity, and availability (CIA); and stakeholder concerns. This chapter has been updated to include more granular use case scenarios in the area of the Advanced Metering Infrastructure.

Conclusion

NISTIR 7628 Rev. 1 presents a comprehensive framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of smart grid stakeholders can use the methods and supporting information presented in this report as guidance for assessing cybersecurity risk and identifying and applying appropriate security requirements.



Additional Resources

NISTIR 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity [3 volumes]:* Vol. 1*, Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements;* Vol. 2*, Privacy and the Smart Grid;* Vol. 3*, Supportive Analyses and References.*

NIST Special Publication 1108R2*, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*, Feb. 2012.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov