Cybersecurity Framework Smart Grid Profile

Workshop: Smart Grid Interoperability and Cybersecurity

November 13-14, 2018

National Cybersecurity Center of Excellence

Information Technology Laboratory, ITL

Engineering Laboratory, EL

This document has been prepared by the Smart Grid Program team comprised of the Smart Grid Program Office in the Engineering Laboratory, along with project participants from the Cybersecurity for Smart Grid Systems project in the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST). This document is a freely available contribution of the Smart Grid Program Office and is published in the public domain.

The ITL promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Executive Summary

The U.S. electric power grid is undergoing modernization to make the grid "smart." While there are clear benefits to the smart grid, the modernization effort is not easy. There will be numerous considerations as power system owners/operators[1] strive to modernize their own capabilities, while also interfacing and co-existing with other power system owners/operators at different stages of the modernization process. And despite the considerable benefits of the future grid, many aspects of the smart grid have cybersecurity risks that need to be considered to ensure a safe, effective grid transformation.

The Smart Grid Profile is an initial attempt to apply risk management strategies from the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework, explained in Section 2) to the smart grid. The Profile provides cybersecurity risk management guidance to power system owners/operators by prioritizing[2] cybersecurity activities based on their effectiveness in helping power system owners/operators achieve common high-level business objectives for the smart grid. These high-level business objectives are:

- Maintain safety
- Maintain power system reliability
- Maintain power system resilience
- Support grid modernization

The Profile also provides power system owners/operators with considerations and challenges they may experience as they implement these cybersecurity activities in infrastructures with high concentrations of distributed energy resources (DERs).

The following are some examples of how power system owners/operators may use the Smart Grid Profile:

- Prioritizing organizational cybersecurity activities that align with available resources
- Referencing the considerations listed for each cybersecurity activity to better manage cybersecurity risk in an environment with high penetration of DERs
- Conveying cybersecurity requirements to an external entity such as a service provider

In Smart Grid environments, power systems owners/operators rely on and interact with a larger community of diverse third parties than in the legacy grid environments. These third parties include but are not limited to vendors, suppliers, contractors, distributed generation owners/operators, and consumers. Many of the cybersecurity activities that power systems owners/operators traditionally implemented within their own infrastructures will need to be extended to the third party-owned devices and infrastructures that interconnect with the power system infrastructure. Furthermore, supply chain risk management considerations are relevant in

[1] In this Profile, "power system owners/operators" refers primarily to distribution grid owners rather than customers and the assets that they own "behind the meter."

[2] The prioritization of cybersecurity activities in this Profile consists of a binary "yes/no" determinations and is discussed in more detail in Section 3

these relationships especially when smart grid devices and systems are interconnecting with third parties. In addition to using the Cybersecurity Framework to help manage risks associated with third parties, power systems owners/operators may consult Cybersecurity Procurement Language for Energy Delivery Systems [10] and Utilities Technology Council (UTC) white paper [11] for more specific guidance.

Notes to Reviewers:

The smart grid is a complex system composed of a large community of diverse parties, each with varied interests and perspectives. This Profile is focused on cybersecurity needs of smart grid owners/operators and therefore may not be sufficiently high level to be useful to all the diverse parties in the smart grid.

The Profile indicates those cybersecurity activities which can directly help power system owners/operators achieve high-level business objectives. However, the Profile's greatest value may be the considerations that power system owners/operators may experience while implementing the cybersecurity activities and in considering how the responsibilities for these considerations change as they modernize equipment and actors in their power systems take on new roles.

Questions for Reviewers:

The prioritization of cybersecurity activities in this Profile is based on high-level business objectives (maintain safety; maintain power system reliability; maintain power system resilience; and support grid modernization) for a smart grid infrastructure with a high-penetration of DER.

- Are these high-level business objectives universal to the smart grid regardless of the architecture[3]?
- What considerations are unique to different grid architectures?
    - Or perhaps unique to specific Functions/Categories (e.g., asset management, maintaining inventory for non-grid devices, etc.) from the Cybersecurity Framework
    - Or perhaps to varied owner/operator perspectives (e.g., merchant transmission owner, cooperative utility, microgrid joint venture between utility and developer, etc.).
- Do you see value in creating additional Risk Profiles to address these considerations, and at what cross-section (e.g., architecture, service level, Functions/Categories, specific physical or market function such as frequency regulation or voltage support, etc.)? If so, why?
- Is the current Risk Profile useful to stakeholders other than power system owners/operators? Should we explore Risk Profiles from the perspective of other smart grid stakeholders, e.g., technology vendors or third-party service providers, and why?

[3] As a high-level description of a grid, architectures define the components, structure, behavior, qualities, properties, and limits of the electric power grid. This Profile explores a High-DER smart grid architecture developed by the Department of Energy's Pacific Northwest National Laboratory (PNNL). PNNL is developing other architectures to express the smart grid.

Table of Contents

List of Appendices

List of Tables

1 Importance of Cybersecurity in the Smart Grid

The US electric power grid has provided inexpensive, reliable power for decades. Even as electric utilities incorporate new technologies and accommodate changing customer expectations, the basic structure of the grid remains broadly consistent with the first electric systems build more than a century ago. In the current grid, power flows in one direction—from centralized generation facilities, through transmission lines, and to customers via distribution utilities. The centralized design has historically brought efficiencies in facilities and operations, but has also made the grid vulnerable to both malicious actions and natural disasters. And new technologies and operational solutions—and their unique vulnerabilities—are becoming more important as evolving demands from economic development and customer expectations come in conflict with the physical constraints of decades old infrastructure.

The US electric power grid is undergoing modernization to make the grid "smart." In contrast to the legacy grid, the Smart Grid will feature intelligent and distributed technologies such as advanced metering infrastructure (AMI) and automated distribution management systems that will enable the grid to incorporate new technologies and resources. By enhancing data utilization at the grid-edge to accommodate bi-directional power flows and other system dynamics inherent to extensive adoption of distributed energy resources (DERs), the grid will become more resilient to disruptions and resilient in the face of attack [3]. As observability and control extend to the grid-edge, customers and other participants will see new economic opportunities through access to wholesale and other energy markets. However, these opportunities carry attendant obligations not previously assigned to customers to support the overall cyber and operational health of the grid.

While the benefits of the smart grid are clear, it will not be an easy modernization effort. Transitioning to the future grid has been compared to the building of the interstate highway system [3]. In the same way that the interstate highway system took decades to complete, modernization of the grid will take coordinated planning and execution that evolves over time. There will be milestones in which the grid will become "smarter," but the full realization of the smart grid may take a decade or more. Along the way, there will be challenges for power system owners/operators as they both strive to modernize their own capabilities while interfacing and co-existing with other power system owners/operators that are at different stages of the transformation process.

The modernized grid will consist of a variety of different architectures. Documenting such architectures to guide smart grid implementation is important when planning for an effort as vast as grid modernization. Grid architectures—using the concepts of system architecture, network theory, and control theory—define the components, structure, behavior, qualities, properties, interactions, and limits of the electric power grid. As a high-level description of a grid, architectures provide several benefits. They help simplify complex grid interactions to understand and reduce risk; provide a shared vision of the future grid; and identify barriers in achieving that vision. The Department of Energy's (DoE) Pacific Northwest National Laboratory (PNNL) is one group developing high-level architectures of the Smart Grid. These architectures describe some of the stages along the grid transformation—from the near-term modernization that still relies on a conventional grid backbone to end states involving extensive automation and high-penetrations of DERs.

Despite the considerable benefits of the future grid, many aspects of the Smart Grid have cybersecurity risks that need to be considered to ensure a safe, effective grid transformation. The modern grid should be safe, reliable and resilient. A resilient grid has to be able to withstand not just hazards, human errors, hardware failure, and software bugs, but also cyber events as well. This document explores evolving grid architectures—including the high DER penetration architecture described by PNNL—and provides guidance for power system owners/operators to manage cybersecurity risks. To that end, the document draws heavily from the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework, discussed in Section 2 below), helping power system owners/operators prioritize those cybersecurity activities that most align with power system goals of safety, reliability, resilience, and grid modernization. The document also provides considerations and challenges that power system owners/operators may face when implementing the cybersecurity activities.

2 Overview of the Cybersecurity Framework

Recognizing the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The EO directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cybersecurity risks to critical infrastructure.

Created through collaboration between industry and government, the Cybersecurity Framework seeks to promote the protection of critical infrastructure. The prioritized, flexible, and risk-based [4]approach of the Cybersecurity Framework helps owners and operators of critical infrastructure manage cybersecurity-related risk. Although it was designed specifically for companies that are part of the U.S. critical infrastructure, many other organizations [5]in the private and public sectors (including federal agencies) are using the Cybersecurity Framework.

The Cybersecurity Framework consists of three main components: the Core, Implementation Tiers, and Profiles.

- The Framework **Core** provides a catalog of desired cybersecurity activities and outcomes [6]using common language. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.

- The Framework **Implementation Tiers** provides context on how an organization views cybersecurity risk management. The Tiers help organizations understand whether they

[4] Risk-based here is differentiated from a compliance-based approach to managing cybersecurity risk. A compliance-based approach often focuses on defining a set of requirements broadly applicable to all organization. A risk-based approach recognizes that each organization has unique threats and risks and enables organizations to prioritize cybersecurity activities according to their environment, requirements, and budgetary considerations.

[5] This document uses the general word "organization" to show that the Cybersecurity Framework may be used by private businesses, government agencies, academia, etc.

[6] The word "outcomes" is used because the Cybersecurity Framework focuses on the "what" not the "how." In other words, the emphasis is on the cybersecurity outcomes that the organization wants to achieve, but not how they will achieve it. The Informative References described on p. 4 help organizations with the "how."

have a functioning and repeatable cybersecurity risk management process and the extent to which cybersecurity risk management is integrated with broader organizational risk management decisions.

- Framework **Profiles** are a customization of the outcomes of the Core to align with an organization’s requirements. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

The Core presents industry standards, guidelines, and practices within five concurrent and continuous **Functions**—Identify, Protect, Detect, Respond, and Recover. Each of these Functions is described below.

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Cybersecurity Framework, enabling an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential cybersecurity event.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable timely discovery of cybersecurity events.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity event.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact from a cybersecurity event.

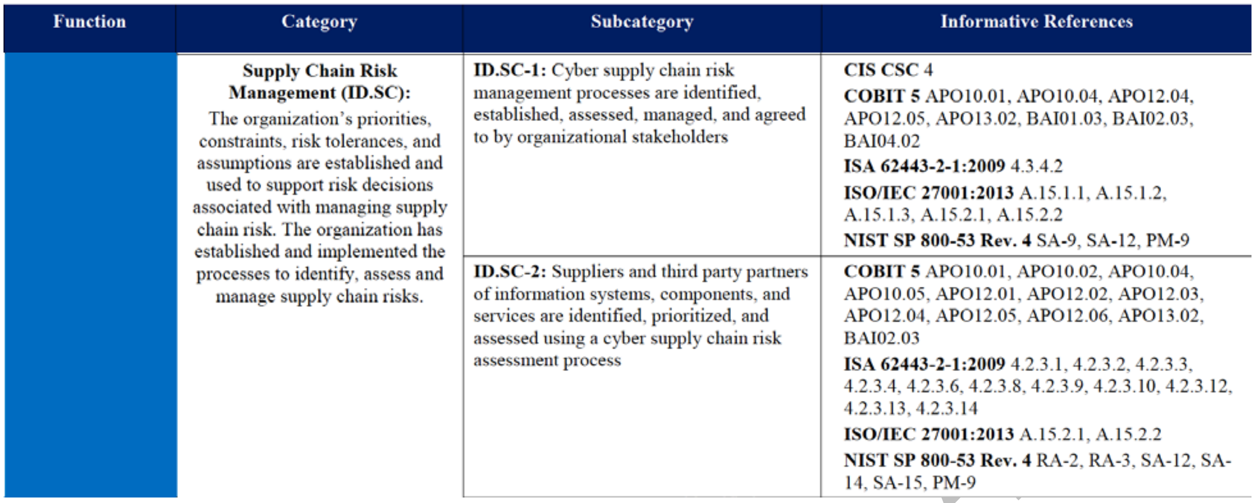
When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying **Categories** and **Subcategories** for each Function. The 108 Subcategories are the discrete cybersecurity outcomes that are organized into 23 Categories like “Asset Management” or “Supply Chain Risk Management.” **Table 1** shows the 5 Functions and 23 Categories of the Core.

Table 1 Cybersecurity Framework Functions and Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

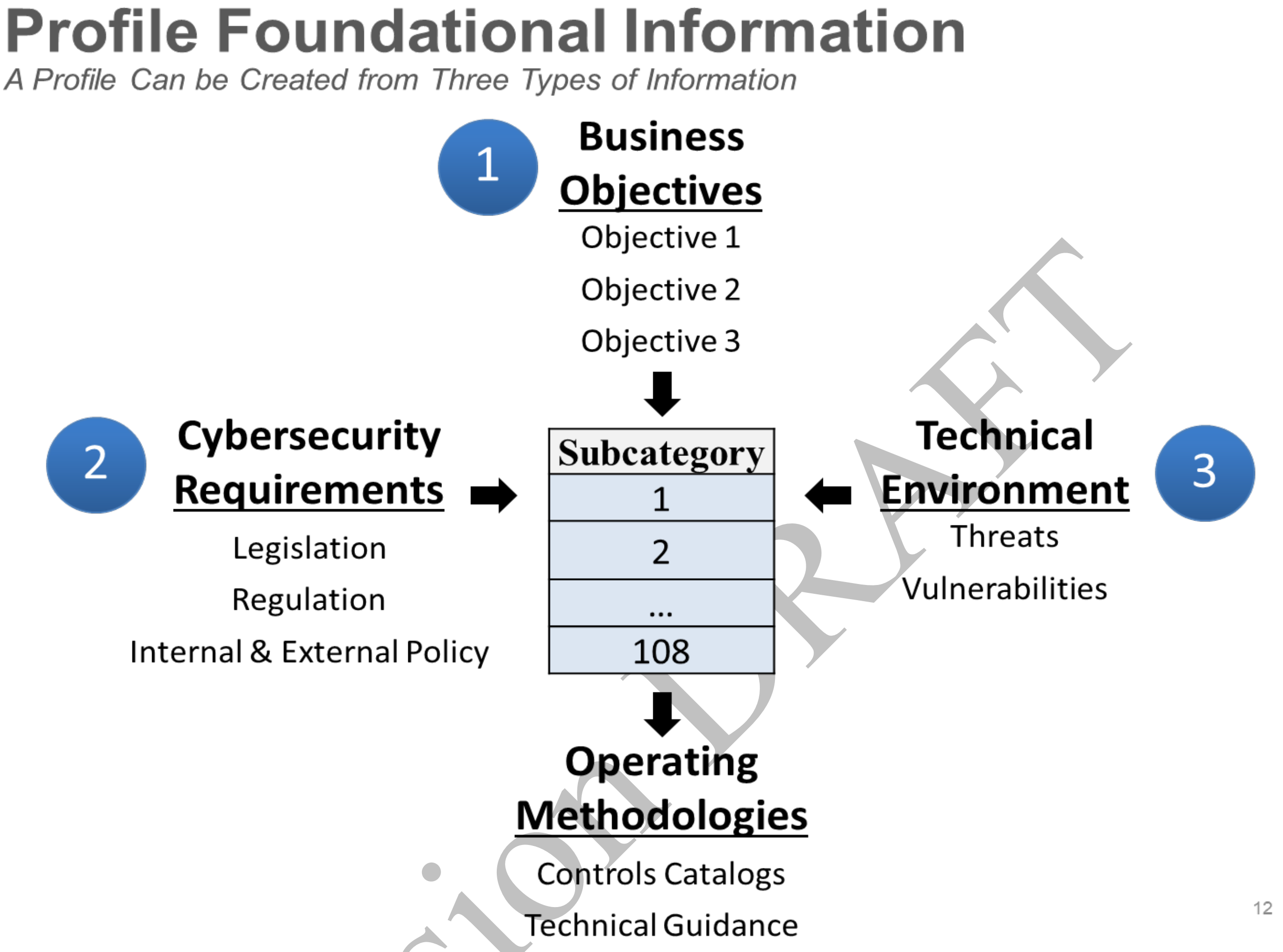
Informative References--such as existing standards, guidelines, and practices—provide practical suggestions for how to achieve the desired outcome of each Subcategory. An example of two Subcategories, along with applicable Informative References, within the Supply Chain Risk Management Category is shown in **Table 2**.

Table 2 Subcategory examples



Function	Category	Subcategory	Informative References
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

Note that the Subcategory outcomes of the Core are organized according to Functions and Categories and are not prioritized. Each organization has unique requirements, risk tolerance, and budget. Therefore, the prioritization of the Subcategory outcomes will vary from one organization to the next. This prioritization of Subcategory outcomes is the essence of a Profile. To create a Profile, an organization considers its high-level business objectives; any cybersecurity requirements through policy, legislation, and regulations; and any unique technical or environmental threats. The organization reviews the Core Categories and Subcategories to determine which outcomes will best help the organization achieve their business objectives, meet cybersecurity requirements, and address their technical and environmental threats. This process is depicted below.



Profile Foundational Information

A Profile Can be Created from Three Types of Information

1 **Business Objectives**

Objective 1

Objective 2

Objective 3

2 **Cybersecurity Requirements**

Legislation

Regulation

Internal & External Policy

Subcategory
1
2
…
108

3 **Technical Environment**

Threats

Vulnerabilities

Operating Methodologies

Controls Catalogs

Technical Guidance

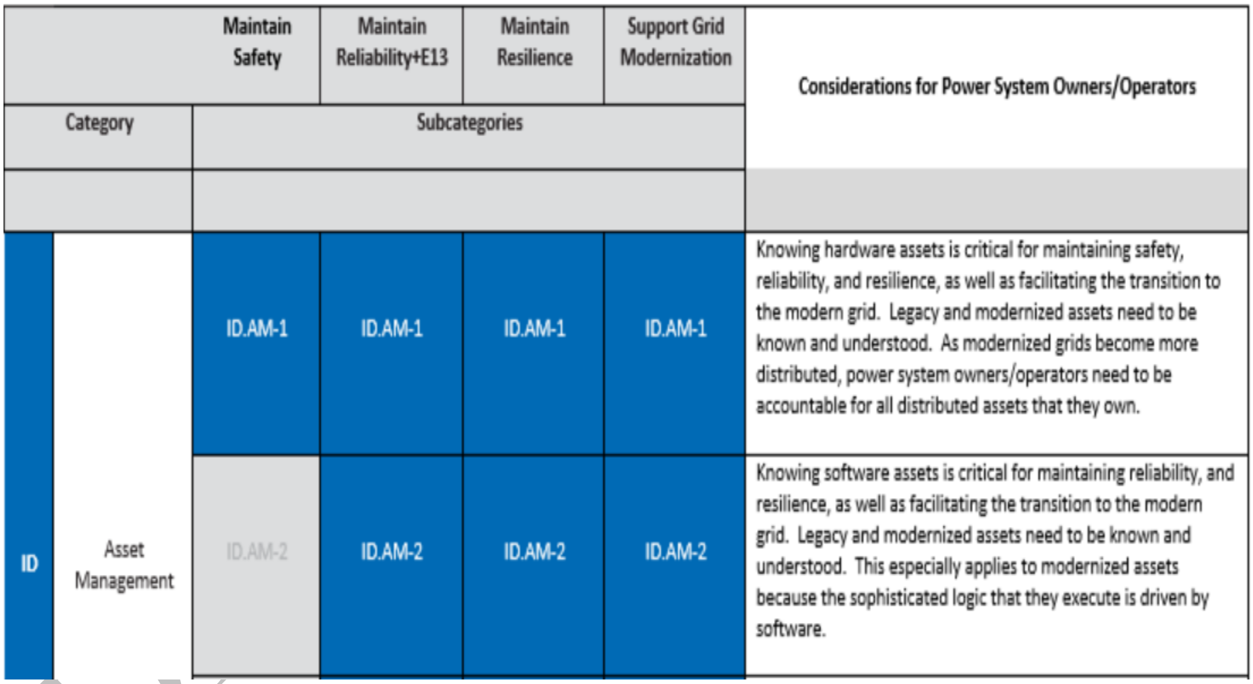
12

Profiles can be created for individual organizations or even parts of an organization (e.g., organizational units such as Finance, Human Resources, or R&D). Increasingly, however, Profiles are being created for entire critical infrastructure sectors (e.g., Financial Services sector) or for sub-sectors (e.g., Oil and Natural Gas sub-sector within the Energy sector). Since organizations within a sector or sub-sector share many of the same business objectives and regulatory requirements, creating high-level Profiles for the sector/sub-sector can provide a common starting prioritization of cybersecurity activities for all organizations within the sector/sub-sector. These Profiles can serve as a starting point, making it easier for organizations to begin incorporating cybersecurity and can also be used to provide a baseline of cybersecurity for organizations within a sector or sub-sector. Individual organizations can take the sector/sub-sector Profile and tailor it to address requirements, business objectives, or environmental considerations unique to them.

3 Smart Grid Profile

The Smart Grid Profile is an initial attempt to create a Profile that is broadly applicable to power system owners/operators of an infrastructure composed of high penetrations of DER. It is intended to help power system owners/operators prioritize[7] cybersecurity activities based on high-level business objectives that are perceived as common throughout the smart grid. The Profile also presents considerations for power system owners/operators as they seek to achieve the outcome of each Subcategory. In addition to providing justifications for a Subcategory's selection, the considerations highlight challenges that power system owners/operators may encounter as they attempt to achieve the Subcategory outcomes. The snippet below from the Profile illustrates considerations for power system owners/operators for Subcategories ID.AM-1 *Physical devices and systems within the organization are inventoried* and ID.AM-2 *Software platforms and applications within the organization are inventoried*.

Table 2 IDENTIFY Smart Grid Profile



		Maintain Safety	Maintain Reliability+E13	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category		Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	Knowing hardware assets is critical for maintaining safety, reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets need to be known and understood. As modernized grids become more distributed, power system owners/operators need to be accountable for all distributed assets that they own.
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	Knowing software assets is critical for maintaining reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets need to be known and understood. This especially applies to modernized assets because the sophisticated logic that they execute is driven by software.

While this Profile is based on business objectives thought to be broadly applicable across the smart grid, individual power system owners/operators may need to tailor their selection of Subcategories. For example, a power system owner/operator may have additional business objectives or may be subject to state or local regulatory requirements not considered in this Profile. These requirements may impact the power system owner/operator's prioritization of

[7] The Subcategory prioritization in this document consists of a binary "yes/no" determination rather than a numerical prioritization (e.g., a rating scale from 1 to 5). Our intent is to identify those cybersecurity outcomes which will directly help power system owners/operators achieve the listed business objectives. More detailed prioritization of Subcategory outcomes will be highly dependent on each organization's unique risk tolerance, requirements, and budget constraints.

Subcategory outcomes.

Development of this Smart Grid Profile consisted of the following steps:

1. Reviewed relevant literature, such as available PNNL smart grid architecture documentation and NIST publications [4], [5], [6], [7].
2. Interviewed industry experts from power system owners/operators and electric power industry think tanks
3. Based on the literature review and the interviews, developed business objectives (discussed in greater detail in Section 4)
4. Analyzed NIST CSF v1.1 Framework Core Subcategories in relation to identified business objectives. Determined whether each Subcategory directly assists power system owners/operators in achieving the business objectives identified in Section 4 of this document.
5. Selected relevant Subcategories, described the rationale for their selection, and composed relevant implementation considerations for power system owners/operators.

The following are some examples of how power system owners/operators may use the Smart Grid Profile:

- Prioritizing organizational cybersecurity activities that align with available resources
- Referencing the considerations listed for each Subcategory to better achieve the outcomes in an infrastructure composed of high penetrations of DERs
- Conveying cybersecurity requirements to an external entity such as a service provider

4 Smart Grid Business/Mission Objectives

Development of the Smart Grid Profile included identification of common business objectives for smart grid infrastructures with high penetrations of DER. These business objectives, which also accounted for regulatory and cybersecurity requirements, provide the necessary context for identifying and managing applicable cybersecurity risks and mitigations. Four common business objectives for power systems stakeholders were identified: *Maintain Safety*; *Maintain Power System Reliability*; *Maintain Power System Resilience*; and *Support Grid Modernization.*

These business objectives are not listed in prioritized order.

Maintain Safety

Safety is an overarching concern of power system management and seeks to minimize the impact of adverse consequences to human life, equipment, and the environment from cybersecurity risks. This requirement aims to manage cybersecurity risks to safety.

Maintain Power System Reliability

Reliability is the ability to deliver stable and predictable power in expected conditions or, in case of power system failure, the ability to restore to a normal operational mode. Reliability addresses both sustained interruptions and momentary interruptions and can be measured in outage duration, frequency of outages, system availability, and response time. Reliability is intended to ensure predictable system performance (the system operates as intended) in sets of predetermined conditions which is defined as the system's expected operating environment. This requirement aims to manage cybersecurity risks to power system reliability.

Maintain Power System Resilience

Resilience is the ability to prepare for and adapt to changing conditions and withstand and gracefully recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Much resiliency engineering focuses on situations where the environmental conditions have deliberately been manipulated by malefactors [8]. This requirement aims to manage cybersecurity risks to power system resilience.

In regard to power systems, resilience is the ability of the system to withstand instability, unexpected conditions or faults, and gracefully return to predictable, but possibly degraded, performance.

Support Grid Modernization

The integration of smart devices into the grid should provide required power to customers, deliver reliable and accurate measurement data to control systems, and cause minimum disruptions in a case of device failure. These smart devices are cyber-physical systems that are increasingly being interconnected to the power distribution system to provide energy and ancillary services. However, distribution power systems were not originally designed to handle dispersed sources of generation, and these advanced systems may not be under direct management of or subject to the security policies and procedures of the power system owner/operator [9]. Additionally, grid modernization efforts will take decades. During this time, legacy and new devices will need to co-exist and interact safely and securely. This requirement supports integration of smart technologies with the legacy grid by managing cybersecurity risks to power system, including integrity and timeliness of data and control commands.

To align cybersecurity activities with overall organizational mission success, Subcategories were identified and prioritized to support these business objectives. This is intended to help power system owners/operators prioritize actions and resources.

The tables below highlight Subcategory outcomes that directly support achieving the identified business objectives. The selection of Subcategories for each business objective was based on a broad range of considerations for Smart Grid architectures. The most critical Subcategories may differ for individual power system owners/operators.

While not all Subcategories were selected for each business objective, users of this document are encouraged to consider all Subcategories in light of their own risk tolerance, risk appetite, asset management approach, and specific business objectives. For the purposes of this document, when a Subcategory is not selected for a specific business objective, it indicates that the activity may not directly assist power system owners/operators in meeting the specific business objective(s).

In developing this profile, the following considerations were identified:

- Most of the Identify Function addresses organizational activities. As a result, most of the Categories and Subcategories within the Identify Function are executed at the organizational level, rather than at a system level or specific security architecture level. These Subcategory outcomes provide overall direction for security activities and apply broadly to all business goals. For this reason, nearly every Identify Subcategory was selected as directly supporting the achievement of the business objectives. Where a Subcategory was not selected, a rationale was provided explaining the decision.

- Regardless of the organization's current infrastructure, the practices in this Profile are good cybersecurity practices to follow. Power system owners/operators will need to review each of the prioritized Subcategories in light of their own risk management processes and determine whether and how those Subcategories apply to their environment. Impact to the sector may differ based on the size of a power system owner/operator, as well as on its infrastructure and interconnectedness. Smaller power system owners/operators should examine each Subcategory in terms of impact to the sector and surrounding communities. While mission-based goals are important, the impact of each Subcategory may be reduced based on the size of the entity and its impact to others. Recommendations should be considered within the context of the mission and the size and interconnectedness of the power system owner/operator.

- In Smart Grid environments, power systems owners/operators rely on and interact with a larger community of diverse third parties than in the legacy grid environments. These third parties include but are not limited to vendors, suppliers, contractors, distributed generation owners/operators, and consumers. Many of the Subcategories that power systems owners/operators traditionally implemented within their own infrastructures will need to be extended to the third party-owned devices and infrastructures that interconnect with the power system infrastructure. Furthermore, supply chain risk management considerations are important in these relationships especially when smart grid devices and systems interoperate with third parties. In addition to using a variety of Subcategories in this document to help manage risks associated with third parties, power systems owners/operators may consult Cybersecurity Procurement Language for Energy Delivery Systems [10] and Utilities Technology Council (UTC) white paper [11] for more specific guidance.

Identify - The Identify Function is critical in the development of the foundation for cybersecurity management, and in the understanding of cyber risk to systems, assets, data, and capabilities. This Function guides the owner/operator in the development of the foundation for cybersecurity management, and in the understanding of cyber risk to systems, assets, data, and capabilities. The activities in Asset Management, Business Environment, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management are the primary security areas that address protections for the four business objectives. The Subcategories below are derived from the Cybersecurity Framework Core, which includes descriptions and informative references for each Subcategory.

Table 3 IDENTIFY Smart Grid Profile

		Maintain Safety	**Maintain Reliability+E13**	**Maintain Resilience**	**Support Grid Modernization**	**Considerations for Power System Owners/Operators**
Category		**Subcategories**				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	Knowing hardware assets is critical for maintaining safety, reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets need to be known and understood. As modernized grids become more distributed, power system owners/operators need to be accountable for all distributed assets that they own.
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	Knowing software assets is critical for maintaining reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets need to be known and understood. This especially applies to modernized assets because the sophisticated logic that they execute is driven by software.

	Maintain Safety	Maintain Reliability+E13	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories				
	ID.AM-3	ID.AM-3	ID.AM-2	ID.AM-3	Understanding communication and data flows is important to ensure reliability and resilience. Communications networks are critical for modernized grids, and understanding the different types of data flows (control, monitoring, and management) will provide critical information for managing those flows within modernized infrastructures and between modernized and legacy infrastructure.
	ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	External information systems may directly impact reliability and resilience. Power system owners/operators need awareness of all power systems, customer-owned devices, and any other third-party systems connected to the distribution system. With respect to supporting grid modernization, legacy and modernized parts of the grid will exist side by side within a single power system owner/operator and across power system ownership lines. Awareness of external information systems that manage both legacy and modernized components is important to assure security of both IT and Operational Technology (OT) infrastructures.
	ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	Resources directly involved in the distribution of power should be prioritized ahead of business systems.
	ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	Identifying all power system stakeholders and their roles and responsibilities with respect to maintaining power and grid restoration is critical to all four business requirements.

	Maintain Safety	Maintain Reliability+E13	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories				
Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	"Supply chain" in this Subcategory includes IT and OT products and services business partners, and other relevant third parties that support power delivery. As such it impacts the reliable flow of power and resiliency efforts including the flow of power from modernized parts of the grid.
	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	The organization's placement in critical infrastructure is especially important to manage potential cascading effects on the sector. The magnitude of potential cascading effects should be understood. Because the modernized grid incorporates distributed generation, the points of integration of distributed resources with the larger grid should be well understood. These pointes of integration may include generation, transmission, distribution, customers, and third-party owners/operators of distributed resources.
	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	Power system owners/operators have a variety of state and local regulatory requirements that should influence their mission and objectives. See ID.GV-3.
	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	Understanding power system dependencies helps maintain reliability and resilience. It also facilitates grid modernization through providing necessary information to plan and implement grid modernization initiatives. Safety is a dependency in the context of this Subcategory which must be identified as such. Identify all sources and loads that require power. Understand information about the loads, sources, and power delivery network at any given time. Use this information to control the flow of power from source to loads.

	Maintain Safety	Maintain Reliability+E13	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories				
	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	The language of this Subcategory specifically highlights resilience.
Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	Information security policy drives a set of coherent security requirements throughout the organization. In this context, security policy should support safety, reliability, resilience, privacy, and other related concerns. Also within this context, grid components are cyber-physical systems (CPS) themselves, composed into a more complex cyber-physical system of systems. NIST CPS Public Working Group (PWG) Framework provides a set of relevant concerns. Organizational informational security policy should address OT and IT environments and how they integrate, the complexity of external partnerships, as well as cover both legacy and modernized environments.
	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	Information security roles and responsibilities and their coordination with external partners directly affect all requirements. In the context of the modernized grid, external parties include the owners of distributed resources.
	ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	This Subcategory is especially applicable in the highly regulated critical infrastructure environment of electric power generation, transmission, and distribution. The modernized grid has additional regulatory requirements that should be considered here.
	ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	Because the grid is a large cyber-physical system, governance and risk management processes should address all risks, not just cybersecurity.

	Maintain Safety	Maintain Reliability+E13	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories				
Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	This Subcategory can be performed as part of a risk assessment. Vulnerabilities from legacy and modernized environments should be included, especially cyber-physical devices in the modern grid.
	ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2	Modernized devices need to be included in information sharing. However, these newer devices that are a part of grid modernization are not yet well-addressed within the information sharing forums of the power system owner/operator community.
	ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3	More threats will be applicable in the more complex environment of the modernized grid, thereby requiring more extensive analysis. The environment is more complex because 1) the high number of devices exponentially increases the attack surface; 2) these devices may have different and distributed ownership; 3) the devices are likely heterogeneous; 4) the overall high interconnectivity of the modernized grid.
	ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4	The modernized grid will have additional and more complex business impacts due to its distributed and multi-owner nature and complex regulatory landscape.
	ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5	Power systems owners/operators should consider threats, vulnerabilities, and impacts to the converged IT/OT environment, including legacy and modernized components.
	ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6	The complexity of the stakeholder landscape in the modernized grid can make the risk responses of power system owners/operators more complicated. Power system owners/operators will need to consider how proposed risk responses will impact interconnected stakeholders.

	Maintain Safety	Maintain Reliability+E13	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories				
Risk Management Strategy	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1	The complexity of the stakeholder landscape in the modernized grid can make risk management processes more complicated.
	ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2	Power system owners/operators should consider the development of a comprehensive strategy to manage risk, including integrating the modernized components of the grid into the determination and description of risk tolerance.
	ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3	Power system owners/operators should consider the potential risk of creating cascading effects on the immediate geographic area, larger region, and the sector overall.
Supply Chain Risk Management	ID.SC-1	ID.SC-1	ID.SC-1	ID.SC-1	Power system owners/operators rely on integrators, ICS vendors, and COTS providers to design and implement networks, systems, and applications that run the grid. As power systems owners/operators modernize their grids, their supply chains increasingly include third party service providers and distributed generation owners/operators. Power system owners/operators therefore need to have robust processes for managing cybersecurity risks stemming from these supply chains that include all relevant members of this diverse ecosystem.
	ID.SC-2	ID.SC-2	ID.SC-2	ID.SC-2	Organizational supply chain risk management processes should be continuously improved regardless of the environment being legacy or modernized.

	Maintain Safety	Maintain Reliability+E13	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories				
	ID.SC-3	ID.SC-3	ID.SC-3	ID.SC-3	Mutually agreeing on a set of appropriate security requirements is important for managing security risks to power systems that transcend organizational boundaries. In addition to security requirements in supplier agreements, power system owners/operators are encouraged to establish a set of security requirements with their third-party partners. These agreements may be mutual, as in power system owners/operators would also be agreeing to a set of security requirements they would commit to abide by. This is a key risk management consideration for power system owners/operators.
	ID.SC-4	ID.SC-4	ID.SC-4	ID.SC-4	Assessments are required to understand whether suppliers and third parties are continuously following agreed-upon cybersecurity requirements. Power system owners/operators should consider that lack of these assurances can have an impact on all critical business/mission goals.
	ID.SC-5	ID.SC-5	ID.SC-5	ID.SC-5	Power system owners/operators should ensure that the modernized (including distributed) power environment is accounted for in response and recovery plans. Testing of these plans helps manage grid modernization efforts. Additionally, suppliers and 3rd-party providers should be included in testing of these plans. Suppliers and 3rd-party providers are critical to orderly restoration after incidents. If they are not properly integrated in testing efforts, it may have an impact on all critical business/mission goals.

Protect – The Protect Function is critical to limit the impact of a potential cybersecurity event. Identity Management and Access Control, Awareness and Training, Information Protection Processes, Maintenance, and Protective Technology are the priority security focus areas. Identity Management and Access Control identifies and regulates personnel ingress and egress. Awareness and Training and the Protection Processes prepare the workforce to achieve cyber security. Protective technology implements security decisions. The Subcategories below are derived from the Cybersecurity Framework Core, which includes descriptions and informative references for each Subcategory.

Table 3 PROTECT Smart Grid Profile

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
PR	Access Control	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1	Identity management is essential for all users, devices, and processes in both legacy and modernized environments.
		PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2	Power system owners/operators should control physical access to the power system, including modernized and distributed grid components. Power system owners/operators should consider the limitations of maintaining physical access to devices on other premises, especially those devices that are owned by a 3rd party.
		PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3	Many grid components are maintained remotely and such access should be secured. For modernized environments, consider the limitations of managing remote access to devices that are owned by a 3rd party, such as distributed resources.
		PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4	Least privilege is important for limiting permissions and authorizations to manage connected devices. This reduces risks of unapproved operations which may create negative impacts to safety, reliability, and resilience. For example, excessive privileges may create an opportunity for compromise during power restoration. Grid modernization efforts should ensure that least privilege principles are designed into and implemented in the modernized grid.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category	Subcategories				
		PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5	Network segmentation is important for containing potential incidents (safety, reliability), and limiting damage from incidents (resilience). Grid modernization efforts should consider segmenting networks from the design stage into operations (e.g., DER devices could be segmented to limit exposure to the rest of the power system infrastructure).
		PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6	In the power system, the safe delivery of reliable power is paramount. For this reason, in case of emergency (e.g., need to restore power), it may be acceptable for power control personnel to share credentials. This sharing will create issues with the binding and proofing of credentials. However, sharing of credentials creates security risks that power system owners/operators will need to manage by implementing mitigating controls or accept the risk.
		PR.AC-7	PR.AC-7	PR.AC-7	PR.AC-7	Connected devices must be authenticated to the grid network. Proper authentication of users, devices, and assets helps ensure safety and reliability. Special care will need to be taken to ensure that modernized devices are also authenticated to the grid network.
	Awareness and Training	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1	User training needs to include a mention that modernization of a grid has impact to cybersecurity. Security awareness training should be provided to all users, including manufacturing system users and managers. Training could include, for example, a basic understanding of the protections and user actions needed to maintain security of the system, procedures for responding to suspected cybersecurity incidents, and awareness of operational security. Also, it is recommended to incorporate threat recognition and reporting into security awareness training.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category	Subcategories				
		PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2	Privileged user training needs to include a mention that legacy to non-legacy migration has impact to cybersecurity.
		PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3	The stakeholder landscape is complicated in the modernized grid and power system owners/operators will need to include roles and responsibilities of all relevant stakeholders, including third parties.
		PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4	Executives need to understand the implications of business decisions (e.g., grid modernization) on cybersecurity—which can impact the larger business/mission goals
		PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5	Training and responsibilities for physical and information security personnel need to be tailored to the unique threats and risks of the grid modernization environment as well as the distributed and multi-owner nature of the environment.
	Data Security	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1	In the case of power grid systems, protecting data-at-rest should apply to protecting the integrity of device settings. If tampered with, device settings may cause a safety or reliability issue.

Category	Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Subcategories				
	PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2	In the case of power grid systems, protecting data-in-transit should apply to protecting the integrity of control information and device settings. If tampered with, device settings may cause a safety or reliability issue. However, power system owners/operators should consider the potential for resource-intensive cryptographic mechanisms to interfere with the functional performance of control systems.
	PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3	Power system owners/operators need to be aware of all distributed, modernization assets they own and manage them throughout the life cycle. IT components embedded in OT devices within the grid modernization infrastructure (e.g., power control and delivery) may present challenges of ownership/contractual agreements with the manufacturers. During disposal of assets, special care should be taken to not explore device configuration data. Note that control data is temporal and therefore does not require protection after it has been acted upon. However, the integrity of device configuration data should be protected to not impact future safety and reliability.
	PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4	Adequate capacity is critical for power system reliability and resilience.
	PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5	Data can be used to mimic system behavior and attack the system. Therefore, protection from data leaks is important for safety and reliability.
	PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6	The integrity of control information and system components is critical to all business/mission requirements.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
		PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7	The separation of development and testing environments is critical to ensure testing does not accidentally impact operational systems. Therefore, insufficient separation could directly impact safety, reliability, and resilience. This applies to both legacy and modernized environments equally; therefore, grid modernization is not specifically highlighted. This should be already done for the legacy environment and this good process should also apply to modernized environments. However, it should be noted that applying this to distributed environments may be challenging due to their scope.
		PR.DS-8	PR.DS-8	PR.DS-8	PR.DS-8	The integrity of power system hardware is critical to safety, reliability, resilience, and grid modernization.
	Information Protection Processes and Procedures	PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1	Baseline configurations are needed for all devices that are owned by a power system owner/operator. However, power system owner/operators should consider that they may have little or no control over the configuration of devices owned by other stakeholders connecting to the grid. Creating and maintaining baseline configurations supports the safety, reliability, and resilience (known state to restore to) of the power grid. Grid modernization efforts are also supported by having a standard configuration for all modernized devices.
		PR.IP-2	PR.IP-2	PR.IP-2	PR.IP-2	Implementing an SDLC ensures quality and predictable performance of systems and networks. It is critical for safety and reliability. While also important for resilience and grid modernization, it is in no way special for those two goals which are thus not selected.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category	Subcategories				
		PR.IP-3	PR.IP-3	PR.IP-3	PR.IP-3	Configuration change control processes support safety, reliability, resilience (known state to restore to), and transition to modernized grid. Power system owners/operators should consider how organizational configuration change control processes will include devices owned by third parties
		PR.IP-4	PR.IP-4	PR.IP-4	PR.IP-4	Backups are essential for retaining device configuration information so that devices can be restored and recovered to proper operational states. Modernized grids are especially susceptible because modern devices have more programmable logic in them. Special consideration should be taken to address backups of devices owned by third parties.
		PR.IP-5	PR.IP-5	PR.IP-5	PR.IP-5	Physical security policies are important for safety and reliability of the power grid. They also support the integration of distributed, modernized devices into the grid.
		PR.IP-6	PR.IP-6	PR.IP-6	PR.IP-6	This Subcategory outcome is not directly applicable to these business/mission requirements because control system data does not have to be confidential.
		PR.IP-7	PR.IP-7	PR.IP-7	PR.IP-7	Protection processes should be continuously improved regardless of whether the power system environment is legacy or modernized.
		PR.IP-8	PR.IP-8	PR.IP-8	PR.IP-8	This Subcategory outcome is not directly applicable to these business/mission requirements.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
		PR.IP-9	PR.IP-9	PR.IP-9	PR.IP-9	Power system owners/operators need to be sure to include the modernized environment/devices in the response and recovery plans and their testing to help manage grid modernization efforts. They must also ensure that the plans address the collaboration between IT and OT personnel and the distributed nature of modernized environments.
		PR.IP-10	PR.IP-10	PR.IP-10	PR.IP-10	Power system owners/operators need to be sure to include the modernized environment/devices in the response and recovery plans and their testing to help manage grid modernization efforts. The plans need to address the collaboration between IT and OT personnel as well as the distributed nature of modernized environments.
		PR.IP-11	PR.IP-11	PR.IP-11	PR.IP-11	Processes and procedures for including cybersecurity in human resources practices are the same for both legacy and modernized environments. Therefore, no special accommodations are required for the modernized grid.
		PR.IP-12	PR.IP-12	PR.IP-12	PR.IP-12	Modernized distributed energy resources can have vulnerabilities that may allow new and unaccounted threat vectors to the power grid. Power system owners/operators should consider how externally-owned devices and third-party owners/operators will be included in a vulnerability management plan.
	Maintenance	PR.MA-1	PR.MA-1	PR.MA-1	PR.MA-1	Special care needs to be taken when devices are owned by third parties as may be the case in modernized environments.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category	Subcategories				
		PR.MA-2	PR.MA-2	PR.MA-2	PR.MA-2	Power system owners/operators need to be aware of any remote access capabilities that the device vendor may have to equipment. This is extremely important in energy environments due to distributed nature, geographical dispersion, and the mission need for remote maintenance of both legacy and modernized devices.
	Protective Technology	PR.PT-1	PR.PT-1	PR.PT-1	PR.PT-1	Audit logs capture information that will be helpful during an attack to find anomalies and potentially limit the impact or stop the incident from inflicting worse damage (helps safety). Capturing and monitoring audit logs is also important for managing cybersecurity risks to grid modernization. These audit logs may provide visibility into the activities and traffic related to these distributed devices.
		PR.PT-2	PR.PT-2	PR.PT-2	PR.PT-2	Protecting and restricting the use of removable media on modernized devices has the same considerations as on legacy environments.
		PR.PT-3	PR.PT-3	PR.PT-3	PR.PT-3	Power system owners/operators should consider how the principle of least functionality will be applied to third-party assets connected to their grid.
		PR.PT-4	PR.PT-4	PR.PT-4	PR.PT-4	Distributed multi-ownership of some modern grid (e.g., DER) environments may make it challenging to protect communications and control networks.
		PR.PT-5	PR.PT-5	PR.PT-5	PR.PT-5	This Subcategory outcome is focused on resilience therefore resilience is selected.

Detect – The Detect Function enables timely discovery of cybersecurity events. Real time awareness and continuous monitoring of the systems is critical to detect cybersecurity events. The Subcategories below are derived from the Cybersecurity Framework Core, which includes descriptions and informative references for each Subcategory.

Table 4 DETECT Smart Grid Profile

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
DE	Anomalies and Events	DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1	A baseline of network operations and expected data flows is extremely important in the OT space because information flows are predictable, and control systems have few users in relation to IT systems. Understanding the control information flows will help monitor and detect unusual network behavior and allow for timely response. This applies equally in legacy and modernized grid environments.
		DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2	Analyzing detected events is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3	When collecting and aggregating data from third-party devices, the devices and the data should be authenticated and validated. Without this authentication and validation, power system owners/operators should carefully consider whether those devices and their data can be trusted.
		DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4	Determining the impact of detected events is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5	Establishing incident alert thresholds is critical for safety, reliability, and resilience. This practice covers both legacy and modernized parts of the infrastructure equally.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
	Security Continuous Monitoring	DE.CM-1	DE.CM-1	DE.CM-1	DE.CM-1	Neglecting to monitor the grid for cybersecurity events may result in missing an event with implications and impact. For grid modernization, monitoring has to be built in for the future. While the selection of safety may be surprising, not monitoring substantially increases the risk of not knowing that there may be safety impacts and being unable to reduce or eliminate them.
		DE.CM-2	DE.CM-2	DE.CM-2	DE.CM-2	Monitoring the physical environment is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.CM-3	DE.CM-3	DE.CM-3	DE.CM-3	Monitoring personnel activity is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.CM-4	DE.CM-4	DE.CM-4	DE.CM-4	Power system owners/operators should consider applying malicious code detection methodologies to both legacy and modernized infrastructure. These devices contain complex software which makes them vulnerable to cyber attacks.
		DE.CM-5	DE.CM-5	DE.CM-5	DE.CM-5	Detecting unauthorized mobile code is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
		DE.CM-6	DE.CM-6	DE.CM-6	DE.CM-6	Power system owners/operators rely on vendors and external service providers for many capabilities, including industrial control systems and communications networks required to operate the grid. Whether service providers are accessing IT or especially OT environments, those activities must be monitored to ensure mitigating actions can be taken in case of attack stemming from external connections.
		DE.CM-7	DE.CM-7	DE.CM-7	DE.CM-7	Unauthorized personnel, connections, devices, or software introduce risks into IT and OT, and may impact grid operations. Any connections to IT and OT systems and networks should be authenticated to ensure that only approved and trusted parties gain access to those systems and networks.
		DE.CM-8	DE.CM-8	DE.CM-8	DE.CM-8	Performing vulnerability scans is required to identify vulnerabilities in critical infrastructure. For modernized environments, power system owners/operators may need to consider an agreement to scan 3rd party-owned devices that are connected to their grid.
	Detection Processes	DE.DP-1	DE.DP-1	DE.DP-1	DE.DP-1	Knowing roles and responsibilities with respect to detection is critical to all four business goals. This includes restoration across power system ownership lines and within a single power system owner/operator with legacy and modernized components and networks. Distributed resources owners/operators may also have a role and responsibilities in detection activities.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
		DE.DP-2	DE.DP-2	DE.DP-2	DE.DP-2	Power system owners/operators need to ensure that detection activities comply with jurisdiction-specific safety requirements.
		DE.DP-3	DE.DP-3	DE.DP-3	DE.DP-3	Power system owners/operators should consider any potential negative impact to the power system due to testing of detection processes. The owners/operators of distributed modernized devices may also need to participate in this testing.
		DE.DP-4	DE.DP-4	DE.DP-4	DE.DP-4	This Subcategory outcome includes communicating detection events across legacy/modernized environments or across owners in the modernized grid.
		DE.DP-5	DE.DP-5	DE.DP-5	DE.DP-5	Detection processes should be continuously improved.

Respond – The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Rapid and effective response and communication to cyber incidents is critical in protecting personnel and environmental safety. Situational awareness to the event unfolding is needed to properly address it. The Subcategories below are derived from the [Cybersecurity Framework Core](), which includes descriptions and informative references for each Subcategory.

Table 5 RESPOND Smart Grid Profile

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
RS	Response Planning	RS.RP-1	RS.RP-1	RS.RP-1	RS.RP-1	This Subcategory outcome applies in both legacy and modernized environments.
	Communications	RS.CO-1	RS.CO-1	RS.CO-1	RS.CO-1	Knowing roles and responsibilities with respect to response and grid restoration is critical to all four business goals. This includes restoration across power system ownership lines and within a single power system owner/operator with integration of legacy and modernized components and networks.
		RS.CO-2	RS.CO-2	RS.CO-2	RS.CO-2	Having an established criterion for reporting incidents helps support safety objectives to ensure that safety considerations are a part of incident response. Furthermore, resilience benefits from a thoughtful criterion.
		RS.CO-3	RS.CO-3	RS.CO-3	RS.CO-3	Assuming that the Subcategory information is shared once an incident has occurred, this Subcategory outcome supports resilience, rather than reliability. Sharing of information is important to ensure safety of restoration crews, and has to be executed across legacy and modernized systems and components.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
		RS.CO-4	RS.CO-4	RS.CO-4	RS.CO-4	Power system owners/operators should consider that the modernized grid is expected to have an expanded set of stakeholders that include distributed resources owners/operators.
		RS.CO-5	RS.CO-5	RS.CO-5	RS.CO-5	Sharing information across utility lines is important, especially when some of the power systems are modernized and some are not. In this context, external stakeholders are assumed to include neighboring power system owners/operators.
	Analysis	RS.AN-1	RS.AN-1	RS.AN-1	RS.AN-1	Investigating notifications from detection systems is important for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		RS.AN-2	RS.AN-2	RS.AN-2	RS.AN-2	Power system owners/operators should take care to understand any similarities and differences in impacts between the legacy and modernized environments.
		RS.AN-3	RS.AN-3	RS.AN-3	RS.AN-3	Performing forensics of incidents is critical for safety and resilience.
		RS.AN-4	RS.AN-4	RS.AN-4	RS.AN-4	Categorizing incidents is critical for safety and resilience.
		RS.AN-5	RS.AN-5	RS.AN-5	RS.AN-5	Having processes for receiving and analyzing vulnerabilities is important for reliability, resilience, and the modernized grid because devices in the modernized grid are smarter than the legacy devices and have their own vulnerabilities. Safety will benefit indirectly from these activities.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category	Subcategories				
	Mitigation	RS.MI-1	RS.MI-1	RS.MI-1	RS.MI-1	Containing incidents is critical for safety and resilience, since once an incident occurs, reliability has already been impacted. Containing incidents is important for both legacy and modernized infrastructures equally.
		RS.MI-2	RS.MI-2	RS.MI-2	RS.MI-2	Mitigating incidents is critical for safety and resilience, since once an incident occurs, reliability has already been impacted. Mitigating incidents is important for both legacy and modernized infrastructures equally.
		RS.MI-3	RS.MI-3	RS.MI-3	RS.MI-3	Newer devices are likely to be more vulnerable because they are smarter. Not patching will hinder the ability of power system owners/operators to be resilient and reliable. Processes should be in place to receive vulnerability information from vendors, as well as to share vulnerability information with device owners/operators across power systems that may have different ownership.
	Improvements	RS.IM-1	RS.IM-1	RS.IM-1	RS.IM-1	Lessons learned will improve future safety, reliability, resilience, and grid modernization.
		RS.IM-2	RS.IM-2	RS.IM-2	RS.IM-2	Updating recovery strategies will improve future safety, reliability, resilience, and grid modernization.

Recover – The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Defined Recovery objectives are needed when recovering from disruptions. The Subcategories below are derived from the Cybersecurity Framework Core, which includes descriptions and informative references for each Subcategory.

Table 6 RECOVER Smart Grid Profile

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
RE	Recovery Planning	RC.RP-1	RC.RP-1	RC.RP-1	RC.RP-1	There are implications to safety of power system owner/operator workers (e.g., linemen) when the recovery plan is executed. The plan should include both legacy and modernized parts of the grid.
	Improvements	RC.IM-1	RC.IM-1	RC.IM-1	RC.IM-1	Incorporating lessons learned into plans is absolutely critical for maintaining reliability and resilience. In this case the other two business goals are of secondary importance.
		RC.IM-2	RC.IM-2	RC.IM-2	RC.IM-2	Updating recovery strategies is critical for reliability and resilience and should cover any activities relevant to safety and grid modernization.
	Communications	RC.CO-1	RC.CO-1	RC.CO-1	RC.CO-1	While important, managing public relations is not critical for the four goals.
		RC.CO-2	RC.CO-2	RC.CO-2	RC.CO-2	While important, repairing reputation is not critical for the four goals.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
		RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3	Recovery activities have to be coordinated to ensure safety of power system owner operator workers (e.g., linemen) working on power recovery. Recovery efforts also require coordination across power systems, some of which may be modernized and some not.

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

AMI	Advanced Metering Infrastructure
CSF	Cybersecurity Framework
DER	Distributed Energy Resources
DoE	Department of Energy
FIPS	Federal Information Processing Standards
ICS	Industrial Control System
IEC	International Electrotechnical Commission
ISA	The International Society of Automation
IT	Information Technology
ITL	Information Technology Laboratory
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OT	Operational Technology
PNNL	Pacific Northwest National Laboratory
UTC	Utilities Telecom Council
UTC	Utilities Technology Council

Appendix B—References

[1] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, https://www.federalregister.gov/d/2013-03915.

[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[3] U.S. Department of Energy, *Smart Grid: An Introduction*, https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf

[4] NISTIR 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity, to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2014, 668 pp. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[5] National Institute of Standards and Technology, Special Publication (SP) 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2015, 247pp. https://doi.org/10.6028/NIST.SP.800-82r2.

[6] Pacific Northwest National Laboratory, J.D. Taft, *Grid Architecture 2*, January 2016, 134 pp. https://gridarchitecture.pnnl.gov/media/white-papers/GridArchitecture2final.pdf

[7] Pacific Northwest National Laboratory, J.D. Taft, *Advanced Networking Paradigms for High-DER Distribution Grids*, version 3.0, May 2016, 30 pp. https://gridarchitecture.pnnl.gov/media/advanced/Advanced%20Networking%20Paradigms%20final.pdf

[8] NIST SP 1500-202, *Framework for Cyber-Physical Systems: Volume 2, Working Group Reports*, Version 1.0. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-202.pdf

[9] IEC TR 62351-12, *Power systems management and associated information exchange – Data and communication security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems*. Edition 1.0, 2016-04

[10] Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language for Energy Delivery Systems*, April 2014, 48 pp. https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

[11] Nadya Bartol, UTC, *Cyber Supply Chain Risk Management for Utilities – Roadmap for Implementation*, 2015, pp. 20. https://utc.org/wp-

content/uploads/2018/02/SupplyChain2015-2.pdf

[12] Avi M. Gopstein, Energy Storage & the Grid—From Characteristics to Impact, Institute of Electrical and Electronics Engineers (IEEE) Proceedings of the IEEE, vol. 100, No. 2, February 2012. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6132596