SMART GRID INTEROPERABILITY PANEL

NISTIR 7628 User's Guide

A White Paper developed by the Smart Grid Interoperability Panel

Smart Grid Cybersecurity Committee

February 2014

Document Source: SGIP Smart Grid Cybersecurity Committee NISTIR 7628 User's Guide Subgroup
Author/Editor: Mark Ellison *et al.*
Production Date: February 26, 2014

Disclaimers

- The information contained in this document is the proprietary and exclusive property of SGIP 2.0, Inc. (SGIP) except as otherwise indicated. No part of this document, in whole or in part, may be reproduced, stored, transmitted, or used for design purposes without the prior written permission of SGIP.
- The information contained in this document is subject to change without notice.
- The information in this document is provided for informational purposes only. SGIP specifically disclaims all warranties, express or limited, including, but not limited, to the implied warranties of merchantability and fitness for a particular purpose, except as provided for in a separate software license agreement.
- This document adheres to the SGIP Intellectual Property Rights (IPR) Policy.

The SGIP

The Smart Grid Interoperability Panel (SGIP) orchestrates the work behind power grid modernization. SGIP was established to identify technical and interoperability standards harmonization that accelerates modernization of the grid. As a member-funded, non-profit organization, SGIP helps utilities, manufacturers, and regulators address standards globally: utilities gain improved regulatory treatment for investment recovery and manufacturers obtain enhanced commercial opportunities worldwide. SGIP members stay competitive, informed and well-connected. To learn more about SGIP, visit http://sgip.org/.

Contents

Tables

Figures

Introduction

In August 2010, NIST collaborated with the Smart Grid Interoperability Panel Cyber Security Working Group (CSWG) to deliver the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*. NISTIR 7628 **was** being updated at the time of the publication of this document. When NISTIR 7628 Revision 1 is finalized, this user's guide will be updated for consistency. The Guideline provides:

- An overview of the cybersecurity strategy used by the CSWG to develop the Smart Grid High-Level Security Requirements;
- A tool for organizations that are researching, designing, developing, implementing, and integrating Smart Grid technologies, whether established or emerging;
- An evaluative framework for assessing risks to Smart Grid components and systems during design, implementation, operation, and maintenance; and
- A guide to assist organizations as they craft a Smart Grid cybersecurity strategy that includes Security Requirements to mitigate cybersecurity and privacy risks.

This NISTIR 7628 User's Guide prepared by the Smart Grid Interoperability Panel Smart Grid Cybersecurity Committee (SGCC) is intended to provide an easy-to-understand approach that you can use to navigate the NISTIR 7628. While NISTIR 7628 covers many significant cybersecurity topics, this User's Guide is focused primarily on the application of NISTIR 7628 Volume 1 in the context of an organization's cybersecurity risk management practices. Although NISTIR 7628 Volume 1 references NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* the electricity subsector has tailored SP 800-39 to meet its unique attributes. This tailored approach is now presented in the *Department of Energy Electricity Subsector Cybersecurity Risk Management Process* ("RMP"), which provides the cybersecurity risk management framework and organizational structure needed before system-specific controls identified in NISTIR 7628 can be applied.

The User's Guide provides an end-to-end implementation guide for your Smart Grid cybersecurity activities. This approach begins with the RMP activities and identification of the Smart Grid Organizational Business Functions, then the associated Mission and Business Processes and the associated Smart Grid systems and assets.

Next the User's Guide identifies and selects the appropriate Smart Grid High-Level Security Requirements needed to protect the Smart Grid systems[1], perform a gap assessment, create a plan to remediate identified gaps, and develop a plan to monitor and maintain Smart Grid high-level security requirements as part of a repeatable risk management process.

This User's Guide is not intended to provide all the detail you will need in a single document. Instead, the User's Guide focuses on the NISTIR 7628 Smart Grid High-Level Security

[1] The term Smart Grid system is used in this document to include information technology (IT) and industrial controls systems (ICS).

Requirements and the Logical Reference Model. The User's Guide leverages the following documents when appropriate to complement the information provided throughout:

- NISTIR 7628, Guidelines for Smart Grid Cyber Security
- DOE Electricity Subsector Cybersecurity Risk Management Process (RMP)
- SGIP Guide for Assessing the Smart Grid High-Level Security Requirements in NISTIR 7628[2]

It should be noted that neither NISTIR 7628, nor this User's Guide imposes any actual requirements on any person or entity.

Electricity Subsector organizations deal with risk every day in meeting their business objectives. These organizations have developed processes to evaluate risk and choose which risks to mitigate and which risks to accept. It is understood that organizations do not have unlimited dollars and resources to implement all of the Security Requirements in the NISTIR 7628 on all of their Smart Grid systems.

Document Structure

This User's Guide contains Activities that include brief descriptions, Steps to complete the Activities, and examples to help you implement the eight Activities detailed below:

Activity 1: Identify Smart Grid Organizational Business Functions

Activity 2: Identify Smart Grid Mission and Business Processes

Activity 3: Identify Smart Grid Systems and Assets

Activity 4: Map Smart Grid Systems to Logical Interface Categories

Activity 5: Identify Smart Grid High-Level Security Requirements

Activity 6: Perform a Smart Grid High-Level Security Requirement Gap Assessment

Activity 7: Create a Plan to Remediate the Smart Grid High-Level Security Requirement Gaps

Activity 8: Monitor and Maintain Smart Grid High-Level Security Requirements

Example artifacts included in the User's Guide are presented as Microsoft Word tables; however, organizations may find it more useful to populate this information in a table or relational database.

Document Audience

Organizations in the diverse community of the Smart Grid—from electric utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use this approach described in this document for assessing risk, and then identifying and applying appropriate NISTIR 7628 High-Level Security Requirements to mitigate that risk.

[2] Links to these documents may be found in the References section.

Activity 1: Identify Smart Grid Organizational Business Functions

The first Activity of the User's Guide is identical to the RMP Tier 1 activities. In this Activity, you will identify the cybersecurity risk governance[3], the high-level Smart Grid Organizational Business Functions from an executive viewpoint, establish the organization's risk tolerance, and identify the organizational cybersecurity risk management strategy.

This is the first opportunity to establish a prioritization to reduce the scope of implementing this User's Guide. For example, in the first iteration of this Activity, you may choose to only select the Smart Grid Organizational Business Functions that are vital to maintaining the Mission and Business Processes of the organization.

Step 1.1: The organization identifies an Executive Sponsor for Cybersecurity Risk Management Governance. At Tier 1 of the RMP, the organizational leadership produces an initial cybersecurity risk management strategy (if one does not already exist) that includes a risk assessment methodology, a risk monitoring strategy, and a cybersecurity governance program. Refer to the RMP, Tier 1, page 23 for Risk Activities. Refer to the RMP, Appendix D for examples of the Governance Models that can be implemented within an organization.

Step 1.2: The Executive Sponsor establishes the Executive Cybersecurity Risk Management Governance Team, which consists of key participants involved in an organization's risk management process. Recognizing that organizations have widely varying missions and organizational structures, there may be differences in naming conventions for risk management-related roles and how specific responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles). However, the basic functions remain the same. Refer to the RMP, Appendix F, page 85, for example roles and responsibilities for this team.

Step 1.3: The Executive Cybersecurity Risk Management Governance Team identifies Smart Grid Organizational Business Functions with respect to Smart Grid strategic goals and objectives (such as Distribution Management, Meter to Cash, etc.).

[3] See the RMP, Appendix D for examples of common governance models.

Table 1 presents an example of the business functions as identified by the Executive Cybersecurity Risk Management Governance Team.

Table 1 – Identify Smart Grid Organizational Business Functions

Example Business Functions
a. Power Operations
b. Metering to Cash
c. Customer Services
d. Corporate Services

Step 1.4: Create an Organizational Business Function Risk Profile Table (in either a spreadsheet or a database). (See Table 2.)

The Executive Cybersecurity Risk Management Governance Team creates a table to identify and prioritize the risks associated with each Organizational Business Function. Add the following columns to the table:

- Organizational Business Functions: Identified in Step 1.3.
- Threats: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations.
- Vulnerabilities: Weaknesses in Smart Grid information systems, cybersecurity procedures, internal controls, or implementations that could be exploited by a threat actor.
- Impact: The degree of loss to an Organizational Business Function operations, assets or individuals that could be expected to have:
  i. a limited adverse effect (Low);
  ii. a serious adverse effect (Moderate); or
  iii. a severe or catastrophic adverse effect (High).
- Probability –The likelihood based on a subjective analysis that a given threat actor is capable of exploiting a given vulnerability.
  i. unlikely to occur (Low);
  ii. likely to occur (Moderate); or
  iii. more than likely to occur (High).
- Constraints – Organizational limitations or restrictions, such as budget, contracts, staff, or regulations.
- Tolerances –A threshold and/or range of acceptable operating risk as defined by the organization.

- Risk Rating –Determine the cybersecurity risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations to organizational operations, organizational assets, or individuals.[4]

  i. a limited risk (Low);
  ii. a serious risk (Moderate); or
  iii. a severe or catastrophic risk (High)

- Risk Responses – The organization evaluates, decides upon, and implements appropriate courses of action to the organization's operations, assets, individuals, and other organizations. If the Executive Cybersecurity Risk Management Governance Team is aware of any existing risk response measures, they may be listed here.[5]

Step 1.5: Perform analysis to determine the Organizational Business Functions you want to focus on based on the analysis that was completed in Step 1.4, and then prioritize the Organizational Business Functions to rank the criticality to the organization. This ranking needs to be determined by each organization based on its own analysis of priority using the risk information that has been provided in this Activity. This ranking recognizes that organizations may not have the resources to address every business function at once and that there may be functions that carry a greater importance to the overall operation of the organization. This step is needed as input for the next Activity.

Table 2 presents an example of how business functions, along with risk information and ranking, were documented by the Executive Cybersecurity Risk Management Governance Team. The initial results produced by the Executive Cybersecurity Risk Management Governance Team determine the Risk Rating of the business functions.

Table 2 – Organizational Business Function Risk Profile

Org. Business Functions	Threats	Vulnerabilities	Impact (H, M, L)	Probability (H, M, L)	Constraints	Tolerances	Risk Rating (H, M, L)	Risk Response	Priority Rating (1, 2, 3…)
Metering to Cash	Disruption of systems used to perform fiscal operations or management	Accessibility of meters and pole top relays.	H Loss of money, time and resources	H Accessibility of equipment	Budget and Financial – How much money can be devoted to this effort this year …or in the future.	We need to manage our current resources more efficiently	H	Make sure there are adequate testing of cyber security controls	1
Power Operations	…	…	…	…	…	…	…	…	…
Customer Services	…	…	…	…	…	…	…	…	…

[4] For more information about determining risk, please see NIST SP 800-30 and the RMP document.
[5] For more information about different types of risk responses (e.g., avoid, accept, transfer, and mitigate), please see the RMP, Section 3.3.2.1.

Org. Business Functions	Threats	Vulnerabilities	Impact (H, M, L)	Probability (H, M, L)	Constraints	Tolerances	Risk Rating (H, M, L)	Risk Response	Priority Rating (1, 2, 3…)
Corporate Services	…	…	…	…	…	…	…	…	…

Activity 2: Identify Smart Grid Mission and Business Processes

This next Activity corresponds to the RMP Tier 2 Activities. In this Activity, you (or the organization) will develop a list of prioritized mission and business processes that support the Organizational Business Functions identified in Activity 1.

Step 2.1: Assemble a group of managers and subject matter experts with responsibilities for the selected prioritized Organizational Business Function(s). Assembling this group will be necessary to complete the following Steps in this Activity.

Step 2.2: Identify the Smart Grid Mission and Business Processes that support and interface with the selected Organizational Business Functions (e.g., Advanced Metering Infrastructure (or smart metering), e-Commerce, Accounting).

An example of this inventory is presented below in Table 3.

Table 3 – Inventory of Mission and Business Processes that Support and Interface with Identified Organizational Business Functions

Prioritized List of Organizational Business Function(s)[6]	Supporting Business Processes (Dependencies)
1. Power Operations	**…**
2. Metering to Cash	a. Advanced Metering Infrastructure (AMI) b. e-Commerce—Billing: Accounts receivable c. Accounting and payroll/Vendor payments
3. Customer Services	…
4. Corporate Services	

[6] The examples provided in the table may not reflect actual prioritization; it serves as an illustrative example only.

Activity 3: Identify Smart Grid Systems and Assets

This Activity corresponds to the RMP Tier 3 activities. In this Activity, you will create (or gather together) a system inventory that supports the mission and business processes identified in Activity 2. The output of this Activity will be a Smart Grid Systems Inventory and a Smart Grid Asset Inventory.

When you determine the impact of the business processes and systems, ensure that the results appropriately align with the business function risk rating.

Step 3.1: Create a Smart Grid Systems Inventory (Table 4) that identifies:

- Selected Organizational Business Functions
- Mission and Business Processes that are inherent and interdependent to the Organizational Business Functions
- Smart Grid System Names that underlay and support the Organizational Mission and Business Processes

Step 3.2: For each system identified in Step 3.1, determine the Risk Prioritization (Low, Moderate, High[7]) for each of the following that were defined in Step 1.4:

- Impact
- Probability
- Risk Rating

Table 4 – Smart Grid Systems Inventory

Priority Business Function(s)	Business Processes	System Name(s)	Risk Prioritization				
			Impact (H, M, L)			Probability (H, M, L)	Risk Ranking (H, M, L)
			C	I	A		
Metering to Cash	a. Advanced Metering Infrastructure (AMI)	AMI Meters	H	H	H	H	H
		AMI Head-End	H	H	H	M	H
		MDMS	H	H	H	M	H
		Billing System	H	L	L	M	H
	b. e-Commerce—Billing: Accounts receivable						
	c. Accounting and payroll/Vendor payments						
…							

[7] Definitions of Low, Moderate, and High are available in Step 1.4.

Step 3.3: Create a Smart Grid Asset Inventory[8] (Table 5) that identifies the following information for each device within a system:

- System name*
- Asset Type*
- Asset Name*
- Location*
- Serial Number
- Logical Addresses (for example, IP Address)
- Firmware (type and version)
- System Addresses (for example, MAC Address)
- Constraints – For example vendor proprietary*
- Additional Threats[9]
- Additional Vulnerabilities*
- Mitigations*

Table 5 – Smart Grid Asset Inventory

System Name	Asset Type	Asset Name	Location	Serial #	Logical Address	Firmware	System Addresses	Constraints	Additional Threats	Additional Vulnerabilities	Mitigations
AMI Meters	Meter ABC	ABC-001	Customer Premise	123456	IP Address A	23.7	123	Flash limited	No locking ring	None	Locked cabinet
	Meter ABC	ABC-002	Customer Premises	234567	IP Address B	34.4	321	Flash limited	None	None	None
	Meter ABC	…	…	…	…	…	…	…	…	…	…
	Field Crew Laptop	Laptop-001	Field Truck A	1000000	IP Address C	23A	400	None	None	None	None
	Field Crew Laptop	Laptop-002	Field Truck B	1000001	IP Address D	23A	401	None	None	None	None
	Field Crew Laptop	…	…	…	…	…	…	…	…	…	…
	Firewall	FW-001	Building-A	2000000	IP Address E	40A	500	None	None	None	None
	Switch	Switch-001	Located in 304 BDT	4000000				None	None	None	None

When identifying the assets, leverage the RMP Case Study document (when released) and the RMP Tier 3 (RMP, page 52) for additional information and guidance on how to identify the assets that support the Smart Grid systems.

[8] While providing all of the following information is ideal, constraints such as program maturity, available resources, etc. impact the level of granularity in the asset inventory. Fields denoted with an * indicate more important data points.

[9] See Step 1.4 or the Glossary (page 27) for additional information.

Activity 4: Map Smart Grid Systems to Logical Interface Categories

This Activity maps the Activity 3, Step 1.3 Smart Grid systems from the Smart Grid Systems Inventory to the Logical Reference Model in NISTIR 7628, Volume 1. In this Activity, you will identify corresponding Actors, Logical Interfaces and Logical Interface Categories (LICs).

Every organization is unique, so portions of the NISTIR Logical Reference Model may not be directly applicable for every business process for every utility. Optionally, instead of solely using the NISTIR 7628 Logical Reference Model diagram, you may create a flowchart that identifies the way the different Actors interface with each other. This will help you conceptualize how the NISTIR 7628 Logical Reference Model aligns to your own organizational business processes.

Step 4.1: Building upon the Smart Grid System Inventory, you will add a new column titled "Actor(s)." For each identified system, review the Logical Reference Model diagram identified in NISTIR 7628 Volume 1, (Figure 2-3, page 17), to determine the associated Actor. See Figure 1, which has sample AMI Actors highlighted.

Note: Your system name and specific terminology used may differ from the Logical Reference Model. Refer to NISTIR 7628, Table 2-1 (page 18), for the description of each Actor.

Step 4.2: Add another column to the Smart Grid Systems Inventory titled "Logical Interfaces." For each Actor identified in Step 4.1, use the Logical Reference Model to document each Logical Interface (e.g., each line between the Actors represents a different Logical Interface, identified by the letter "U" and number such as U24).

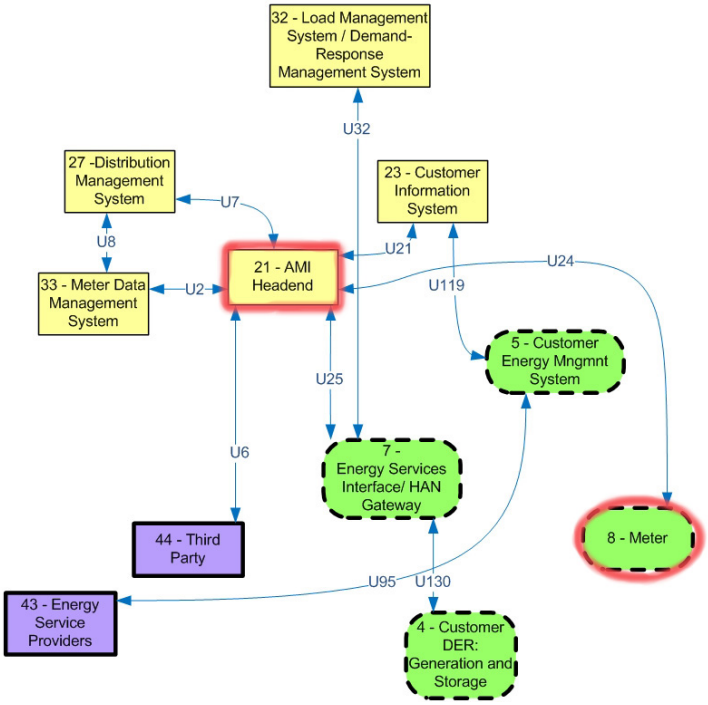


Figure 1 – NISTIR 7628 Logical Reference Model Sample

Step 4.3: Add an additional column to the Smart Grid Systems Inventory titled "Logical Interfaces Category(s)." For each Logical Interface identified in Step 4.2, select the corresponding Logical Interface Category using NISTIR 7268, Volume 1, Table 2-2, Logical Interfaces by Category (pages 27-29). (e.g., U24 belongs to Logical Interface Category 18: Interface between metering equipment.) Table 6 provides an example of a Smart Grid Systems Inventory that includes sample Actors, Logical Interfaces, and LICs.

Table 6 – Smart Grid Systems Inventory with Actor(s), Logical Interfaces, and LIC(s)

Priority Business Function(s)	Business Processes	System Name(s)	Prioritization					Actor(s)	Logical Interfaces	Logical Interface Category(s)
			Impact (H, M, L)			Probability (H, M, L)	Risk Ranking (H, M, L)			
			C	I	A					
Metering to Cash	**a.** Advanced Metering Infrastructure (AMI)	AMI Meters	H	H	H	H	H	8	U24 U64 U35 U41 U47 U80 U120	18 18 17 18 18 6 15
		AMI Head-End	H	H	H	M	H	21	U24	18
		MDMS	H	H	H	M	H	33	U2	7
		Billing Sys	H	L	L	M	H	42	U64	18
	b. e-Commerce—Billing: Accounts receivable									
	c. Accounting and payroll/Vendor payments									
…										

Activity 5: Identify Smart Grid High-Level Security Requirements

This Activity identifies the recommended Smart Grid High-Level Security Requirements associated with each Logical Interface Category (LIC) identified in the previous step.

Below is an approach that utilizes the LIC tables to identify the Smart Grid High-Level Security Requirements.

Step 5.1: Building on the Smart Grid Systems Inventory from Activity 4, Step 4.3, add a new column titled "NISTIR CIA Impact." This will identify the CIA Impact level, as defined in NISTIR 7628, associated with each LIC identified in the previous step. Use Figure 2 (Smart Grid Impact Levels from NISTIR 7628, Table 3-2), to identify the CIA impact level for each LIC.

Logical Interface Category	Confidentiality	Integrity	Availability
1	L	H	H
2	L	H	M
3	L	H	H
4	L	H	M
5	L	H	H
6	L	H	M
7	H	M	L
8	H	M	L
9	L	M	M
10	L	H	M
11	L	M	M
12	L	M	M
13	H	H	L
14	H	H	H
15	L	M	M
16	H	M	L
17	L	H	M
18	L	H	L
19	L	H	M
20	L	H	M
21	L	H	L
22	H	H	H

Figure 2 – Smart Grid Impact Levels

Step 5.2: Add an additional column to the Smart Grid Systems Inventory titled "Organizational CIA" with three columns, one for Confidentiality, one for Integrity, and one for Availability. (See Table 7 below.) The purpose of this step is to review the NISTIR-provided CIA designations against the organization's own risk determinations.

It is possible based on an organization's risk assessment results to modify the NISTIR-provided CIA Impact Levels for your implementation. This step results in the selection and determination of the best CIA ranking between the Impact Analysis

done in Activity 3, Step 3.2 and the NISTIR CIA Impact identified in Step 5.1 above. This Organizational CIA is an opportunity to reconcile what the organization believes is the CIA and what the NISTIR has designated as the CIA.

Optionally, if you would like to better visualize the connections and risks associated with the LIC CIA impacts, you can reference the LIC flow charts (NISTIR 7628, pages 33-77). Note: Your organization's architecture may be different than what is shown and this may need to be taken into consideration when identifying the LIC CIA impacts.

Table 7 – Smart Grid Systems Inventory with CIA Impacts

System Name(s)	Risk Prioritization					Actor(s)	Logical Interfaces	Logical Interface Category(s)	NISTIR CIA Impact			Organizational CIA impact		
	Impact (H, M, L)			Probability (H,M,L)	Risk Ranking (H,M,L)									
	C	I	A						C	I	A	C	I	A
AMI Meters	H	H	H	H	H	8	U24	All GRC						
								All CTR						
								18	L	H	L	L	H	L
							U35	All GRC						
								All CTR						
								17	L	H	M	L	H	M
AMI Head-End	H	H	H	M	H	21								
MDMS														
…														

Step 5.3: In this step, add two additional columns to the Smart Grid Systems Inventory titled "Requirement Type" and "Requirements for Each System" (See Table 8 below). Governance, Risk and Compliance (GRC) Requirements, while centered around policy, procedure, and compliance-based activities, are intended to be addressed at the organization level. Add "GRC" to the "Requirement Type" column. GRC requirements are applicable for all of the system's LICs and may be inherited from the organizational-level.[10]

Using NISTIR 7628, Volume 1, Table 3-3 Allocation of Security Requirements to Logical Interface Categories, (Page 79), identify each of the GRC Smart Grid Requirements based on your Risk Ranking for the system in the Smart Grid Systems

[10] Security requirements are inheritable by Smart Grid information systems or Smart Grid information system components when these systems/components receive protection from requirements, but the requirements are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system/component.

Inventory. These are the white shaded rows in Table 3-3. (See Figure 4 for an example of the NISTIR 7628 Table 3-3.) The identified GRC requirements will populate the next column, "Requirements for Each System."

For example, in Table 8, we identify SG.AC-1 as a GRC requirement for the AMI meter system because this requirement is applicable to systems of all risk rankings.

Dark Gray = Unique Technical Requirement
White = Common Governance, Risk and Compliance (GRC)
Light Gray = Common Technical Requirement

Smart Grid Requirement Number	Logical Interface Categories																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.AC-1	Applies at all impact levels																					
SG.AC-2	Applies at all impact levels																					
SG.AC-3	Applies at all impact levels																					
SG.AC-4	Applies at all impact levels																					
SG.AC-6	Applies at moderate and high impact levels																					
SG.AC-7	Applies at moderate and high impact levels																					
SG.AC-8	Applies at all impact levels																					
SG.AC-9	Applies at all impact levels																					
SG.AC-12							H	H									L				L	H
SG.AC-13																	M		M			
SG.AC-14	H	H	H	H	H	H	M	M	M	H			H	H	M	M	H	H		H	H	H
SG.AC-15																				H	H	H

Figure 3 – Table 3-3 Allocation of Security Requirements to Logical Interface Categories from NISTIR 7628 Example

Step 5.4: The Common Technical Requirements (CTRs) are the technical requirements that are applied against all of the LICs. Add "CTR" to the "Requirements Type" column in Table 8. CTRs should be allocated to each Smart Grid system and not necessarily to every component within a system, as the focus is on security at the system level. Using NISTIR 7628, Table 3-3 (these are the light grey shaded rows in Table 3-3), identify each of the CTRs based on your Risk Ranking from Activity 3, Step 3.2, for the system in the Smart Grid Systems Inventory. Add these CTRs to the "Requirements for Each System" column.

For example, in Table 8 we identify SG.AC 6 as a CTR for the AMI meter system because the system has a Risk Ranking of High and the requirement applies to systems with Moderate- and High-risk rankings.

Step 5.5: Unlike the previous two categories of requirements, the Unique Technical Requirements (UTRs) are allocated to one or more of the LICs.[11] UTRs also should

[11] Unique Technical Requirements are specialized technical requirements that may not be feasible or necessary to implement for every LIC.

be allocated to each Smart Grid system and not necessarily to every asset within a system, as the focus is on security at the system level.

Using NISTIR 7628's Table 3-3, identify each of the UTRs based upon your Risk Ranking for the system in the Smart Grid Systems Inventory and the appropriate LIC identified for each system. These are the dark grey shaded rows in Table 3-3. For each LIC with UTRs, list all of the UTRs in the "Requirements for Each System" column.

For example, in Table 8 we identify SG-AC-14 as a UTR for the AMI meter system LIC 18 because the AMI Meter system has a risk ranking of High and Figure 4 indicates that this requirement is applicable if it has a risk ranking of High.

Step 5.6: For each Requirement listed in the Smart Grid Systems Inventory (see Table 8), refer to the Security Requirement Descriptions in the NISTIR 7628, pages 90 – 209 to identify if there is an enhancement for the requirement. (See Figure 4 for an example.) Even though this example is for a UTR, the process is the same for all three types of Requirements. If a Requirement has a Requirement Enhancement section (See Figure 4), compare the Impact Level Allocation for the High, Moderate, and Low-level impacts, which are located at the bottom of the Requirement Description with the applicable Organizational CIA Ratings in the Smart Grid Systems Inventory.

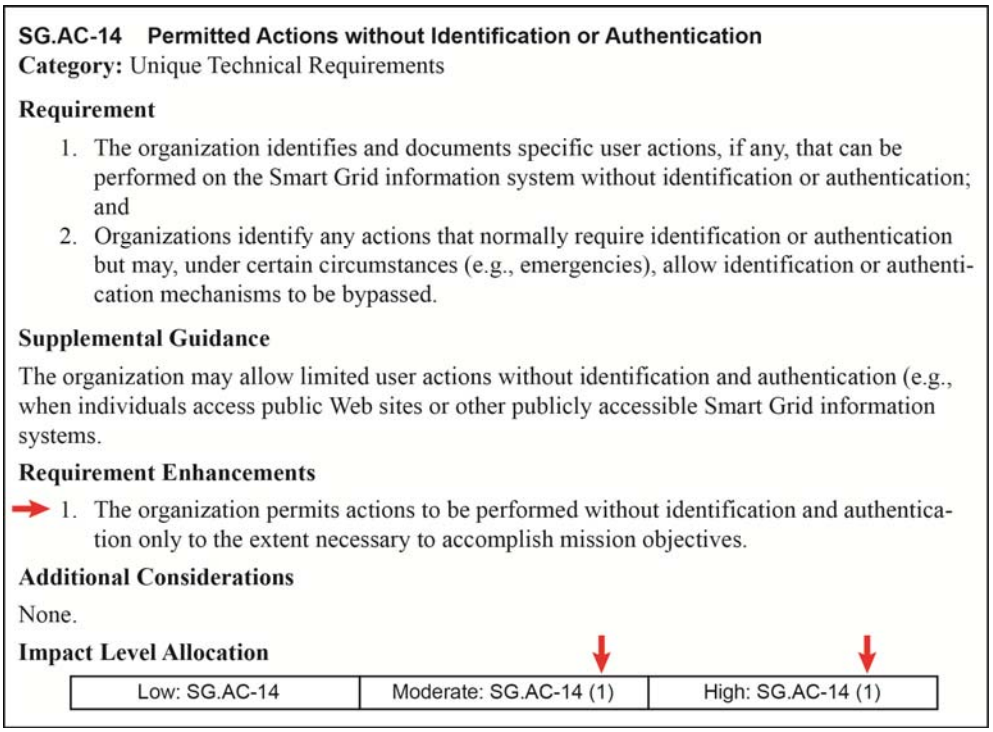
NISTIR 7628, Table 3-3 identifies if there are any requirement enhancements that are applicable to GRC and CTRs at different impact levels. Unique Technical Requirements may also have associated requirement enhancements, but they are not listed in Table 3-3 due to space constraints.

For example, in Figure 4, SG.AC-14 has a Requirement Enhancement if the Impact Levels for any LIC associated with a system rated at High or Moderate. In Step 5.1 we determined that LIC 18 had the Integrity Impact of High, which most closely applies to this requirement; therefore, we need to apply this SG.AC-14 requirement enhancement for AMI Meters System.

In the Smart Grid Systems Inventory (Table 8), we determine that the AMI system has an Organizational CIA Impact Integrity rating of High and Integrity is applicable to requirement SG-AC-14. Therefore, the requirement enhancement for this requirement is applicable to the AMI meters in Table 8.

To be consistent with the NISTIR 7628, enter applicable requirement enhancements (within parentheses) next to the applicable requirements. For example, the entry for SG.AC-14 in the "Requirements for Each System" column would be updated to "SG.AC-14 (1)."

Step 5.7: Finally, add another column to the Smart Grid Systems Inventory (Table 8) titled "Consolidated UTR Requirements for Each System." In this column consolidate all of the UTRs for a system together from all of the LICs listed for that system. (See Table 8 for an example.)



SG.AC-14 Permitted Actions without Identification or Authentication

Category: Unique Technical Requirements

Requirement

1. The organization identifies and documents specific user actions, if any, that can be performed on the Smart Grid information system without identification or authentication; and
2. Organizations identify any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed.

Supplemental Guidance

The organization may allow limited user actions without identification and authentication (e.g., when individuals access public Web sites or other publicly accessible Smart Grid information systems.

Requirement Enhancements

1. The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-14	Moderate: SG.AC-14 (1)	High: SG.AC-14 (1)

Figure 4 – Smart Grid High-Level Security Requirement Description

Table 8 – Smart Grid Systems Inventory with CIA Impacts, Unique Technical Requirements, and Requirement Enhancements

System Name(s)	Risk Prioritization: Impact (H, M, L) C	I	A	Probability (H,M,L)	Risk Ranking (H,M,L)	Actor(s)	Logical Interfaces	Logical Interface Category(s)	NISTIR CIA Impact C	I	A	Organizational CIA impact C	I	A	Requirement Type	Requirements for Each System	Consolidated UTR Reqs. For each system
AMI Meters	H	H	H	H	H	8	All	All							GRC	SG.AC-1 SG.AC-2 SG.AC-3 SG.AC-4 … …	SG.AC-12 SG.AC-13 SG.AC-14 (1) SG.IA-4 SG.IA-5 SG.IA-6 SG.SC-26 SG.SC-29 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8 SG.SC-9 SG.SI-7
							All	All							CTR	SG.AC-6 SG.AC-7 SG.AC-8 SG.AC-9 … …	
							U24	18	L	H	L	L	H	L	UTR	SG.AC-14 (1) SG.IA-4 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-26 SG.SI-7	
							U35	17	L	H	M	L	H	M	UTR	SG.AC-12 SG.AC-13 SG.AC-14 SG.IA-4 SG.IA-5 SG.IA-6 SG.SC-29 SG.SI-7	
AMI Head-End																	
MDMS																	
…																	

Activity 6: Perform a Smart Grid High-Level Security Requirement Gap Assessment

In this Activity, you will review the Smart Grid System Asset Inventory and the Smart Grid Systems Inventory to determine if each Smart Grid High-Level Security Requirement has been implemented for each of the system's assets. Identified gaps will be documented in the Smart Grid Systems Inventory.

For additional information on conducting security requirements assessments, refer to the SGIP *Guide for Assessing the High-Level Security Requirements in NISTIR 7628.*

Step 6.1: Add a column to the Smart Grid Systems Inventory titled "Assessment Ratings (S or O)." (See Table 9.) This column will be used to identify how well each requirement is applied to each of the systems identified in the Smart Grid Systems Inventory (Table 9), and you will enter one of the two following Assessment Ratings in the Smart Grid Systems Inventory:

S – For Satisfied or O – For Other than Satisfied[12]

Step 6.2: Using the Smart Grid Asset Inventory (Table 5) from Activity 3, Step 3.3, and the Smart Grid Systems Inventory (Table 8) from Activity 5, conduct the gap assessment to validate how well the implemented security requirements match the Smart Grid High-Level Security Requirements for each system as identified in Table 9.

The methodologies for conducting the Gap Assessment are identified in the SGIP document *Guide for Assessing the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cybersecurity*, Section 4, pages 18-25. The Assessment Guide provides a set of guidelines for building effective security assessment plans and a baseline set of procedures for assessing the effectiveness of security requirements employed in Smart Grid information systems.

Step 6.3: Add a column to the Smart Grid Systems Inventory titled "Assessment Gaps." If the result of the gap assessment is "Other than Satisfied," provide a short description of the gap next to the associated Smart Grid High-Level Security Requirements for each system.

Depending on the security requirement, it may be necessary for you to review how well requirements are applied to each of the assets associated with the identified system. The decision to do so depends on details of the LIC and professional judgment. In many cases, the decision to go to the asset level is clear as the LIC deals with individual assets in the field. When performing an assessment for systems and assets, do not lose sight of how they are all interconnected and their dependencies.

[12] An assessment finding of Satisfied (S) indicates that the requirement has been met producing a fully acceptable result. An assessment of Other than satisfied (O) indicates potential anomalies in the operation or implementation of the requirement that may need to be addressed by the organization.

The example provided below in Table 9 leverages the assessment method outlined in the NISTIR 7628 Assessment Guide. Each organization may leverage its own method for determining security requirement gaps and apply that methodology to complete this Activity.

Table 9 – Smart Grid Systems Inventory with Assessment Scores, Assessment Gaps

System Name(s)	…	Logical Interface Categories (LICs)	…	Requirement Type	Reqs. for each system	Consolidated UTR Reqs. For each system	Assessment Ratings (S or O)	Assessment Gaps
AMI Meters	…	All		GRC	SG.AC-1 SG.AC-2 SG.AC-3 SG.AC-4		S S S S	
		All		CTR	SG.AC-6 SG.AC-7 SG.AC-8 SG.AC-9		S S S S	
		18		UTR	SG.AC-14(1) SG.IA-4 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-26 SG.SI-7	SG.AC-14(1) SG.IA-4 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-26 SG.SC-29 SG.SI-7	S S S O S O S S S S S	SC-5: No network perimeter devices. SC-7: No monitoring of boundary communications.
		17		UTR	SG.AC-14 (1) SG.IA-4 SG.IA-5 SG.IA-6 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-26 SG.SC-29 SG.SI-7			
AMI Head- End		…		…	…		…	…
MDMS		…		…	…		…	…
…								

Activity 7: Create a Plan to Remediate the Smart Grid High-Level Security Requirement Gaps

In this Activity, you will develop a plan to mitigate the identified Smart Grid High-Level Security Requirement Gaps from Activity 6. As part of the mitigation you will evaluate how the "Other than Satisfied" requirements need to be addressed. This Activity corresponds with the Risk Response activity in the RMP Tier 3 (pages 55-57). Risk response actions—whether Risk Acceptance, Risk Avoidance, Risk Sharing, Risk Transfer, Risk Mitigation or a combination of these responses—should be approved according to your organization's risk management practices. This is also the area where the risk decision to omit or enhance a requirement can be documented.

Examples of valid determinations for removing a Smart Grid High-Level Security Requirement include compensating security requirements are in place or the cost to mitigate exceeds the impact of a compromise. The next step is to identify mitigations, prioritize them logically, and craft plans to address them. Where necessary, you'll need to leverage your organization's risk acceptance processes in conjunction with prioritizing the planning.

Step 7.1: Add a column to the Smart Grid Systems Inventory titled, "Proposed Mitigations." (See Table 10.) This column will be used to document the Risk Response actions associated with each "Other than Satisfied" Assessment Rating. Refer to the RMP Tier 3 (pages 55-57) for more information. Additionally, provide a short explanation in this column about why your organization chooses the specific Risk Response Action(s).

Step 7.2: Add a column to the Smart Grid Systems Inventory titled "Priority." This column will be used to document mitigation priorities. To begin prioritizing the mitigations, start with the list of Organizational Business Functions from Activity 2 and the list of Mission and Business Processes from Activity 3.

Step 7.3: Using the Prioritized Organizational Business Functions and Prioritized Mission and Business Processes, determine a Mitigation Priority (for example Low, Moderate, or High) based on the following characteristics identified in Activity 1, Step 1.3, and Activity 3, Step 3.2:

- Threats
- Vulnerabilities
- Potential Impact
- Probability
- Constraints
- Tolerances
- Risk Rating

Entities can determine for themselves which scale to use (e.g. Low, Moderate, High or a numbered scale (1-5), etc.).

Consider the following questions when prioritizing the gaps for action:

- Which gaps are most important in the context of the organization's objectives?
- Which gaps are most important in the context of the organization's role in critical infrastructure?
- Can the necessary resources be made available to address the gap?
- Are there efficiencies that can be realized by addressing the gap? (i.e., efficiencies may include streamlining controls or compliance activities.)

When prioritizing gaps, it is important to consider time, costs, and risks associated with closing the

Step 7.4: Using the determination made in Step 7.3, you can assign a priority to each of the Proposed Mitigations that fits your risk tolerance. Consider how gaps should be prioritized, which may be based on resource requirements and availability (cost, level of effort, time to complete). This way, an appropriate timeline for mitigation can be developed and met consistent with longer term planning and budgeting by your organization.

Step 7.5: Once the identified gaps are prioritized, develop plans to address selected gaps. Table 10 shows the Smart Grid Systems Inventory with proposed mitigations and priorities.

Table 10 – Smart Grid Systems Inventory with Proposed Mitigations and Priorities

System Name(s)	LICs		GRC Req. for each system	Consolidated UTRs	Assessment Ratings (S or O)	Assessment Gaps	Proposed Mitigations	Priorities (H, M, L)
AMI Meters	All	GRC	SG.AC-1 SG.AC-2 SG.AC-3 SG.AC-4		S S S S			
	All	CTR	SG.AC-6 SG.AC-7 SG.AC-8 SG.AC-9		S S S S			
	18	UTR	SG.AC-14(1) SG.IA-4 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-26 SG.SI-7	SG.AC-14(1) SG.IA-4 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-26 SG.SC-29 SG.SI-7	S S S O S O S S S S	SC-5: No network perimeter protection devices. SC-7: No monitoring of boundary communications	SC-5: Install a firewall and IDP. SC-7: Install SIEM to receive alerts from IDP.	H H
	17	UTR	SG.AC-14 (1) SG.IA-4 SG.IA-5 SG.IA-6 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-26 SG.SC-29 SG.SI-7…					
AMI Head-End	…	…	…	…	…	…	…	
MDMS	…	…	…	…	…	…	…	
…	…	…	…	…	…	…	…	

Activity 8: Monitor and Maintain Smart Grid High-Level Security Requirements

Deviations from the assessment will occur over time from a number of factors including environmental changes that include systems changes, new threats and vulnerabilities, and/or changes to your organization's business risk profile. Changes can also occur at the Organizational Business Function and Mission and Business Process levels.

Step 8.1: Develop a plan to monitor the progress of Activity 7, Step 7.5. Refer to the RMP Tier 3 Risk Monitoring step for more information on implementing a Cybersecurity Mitigation Plan at the system and asset level.

Step 8.2: Leverage your change management system to identify when significant changes are made to Smart Grid Systems or Assets. When significant changes are made to existing systems, re-complete the Steps in Activities 6 and 7. All of the Activities need to be followed before a new system is put into production.

Implementation Tips:

- The ongoing monitoring of systems' security posture can be done by utilizing automated tools and following documented processes.
- Periodically conduct systems evaluations to identify any new cybersecurity issues.
- Reevaluate in response to major changes in the business, technology, market, or threat environments to ensure that the current profile matches the organization's desired state.

Glossary

Asset - A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems [NISTIR 7298 Rev. 2]

Asset Type - Organizing of assets into common groups of software and hardware.

Availability - Ensuring timely and reliable access to and use of systems, assets, and information.

Also

Ensuring a system is accessible and useable upon demand by an authorized entity.

Business Process - A collection of related, structured activities, systems, and/or services that contribute to an Organization's Business Functions.

Confidentiality - Ensuring that sensitive information is not disclosed to unauthorized individuals, entities, or processes. Also ensuring that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.

Constraints - Organizational limitations or restrictions, such as, budget, contracts, staff, or regulations.

Impact - The degree of loss to an Organizational Business Function operations, assets or individuals that could be expected to have:

i. a limited adverse effect (Low);
ii. a serious adverse effect (Moderate); or
iii. a severe or catastrophic adverse effect (High).

Also

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [NISTIR 7298 Rev. 2; CNSSI-4009]

Industrial Control System - An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and

	smaller control systems using programmable logic controllers to control localized processes. [NISTIR 7298 Revision 1; SP 800-53; SP 800-53A; SP 800-39; SP 800-30]
Information System -	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.] [NISTIR 7298 Revision 2; SP 800-53; CNSSI-4009]
Integrity -	Ensuring that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Organizational Business Functions -	Those business functions vital to maintaining the core business activities of the organization. The Executive Cybersecurity Risk Management Governance Team identifies Smart Grid related Organizational Business Functions with respect to Smart Grid strategic goals and objectives (such as Distribution Management, Meter to Cash, etc.).
Probability -	The likelihood based on a subjective analysis that a given threat actor is capable of exploiting a given vulnerability.
Risk -	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [NISTIR 7298 Rev. 2; FIPS 200]
Risk Rating -	Determination of the cybersecurity risks based on a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations to organizational operations, organizational assets, or individuals.[13]

[13] For more information about determining risk, please see NIST SP 800-30 and the RMP document.

Risk Response - Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. [NISTIR 7298, Revision 2; SP 800-30; SP 800-39]

Also

Course of actions regarding the organization's operations, assets, individuals, and other organizations which are implemented based upon their evaluation of Risk, Probability and Impact and related course of action decisions.

Risk Tolerance - A threshold and/or range of acceptable operating risk as defined by the organization in order to achieve a potential desired result.

Smart Grid - The application of end-to-end automation technology, bi-directional programmatic logic, and advanced telecommunications infrastructure integrated into traditional electric transmission and distribution systems to improve operations, maintenance, and planning for existing grid capabilities and to provide new capabilities through introduced technology and connectivity.

System - A collection of related hardware and software assets that participate in the Smart Grid. For example, many of the Actors found in NISTIR 7628's Logical Reference Model are systems.

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations.

Also

The potential for a threat-source to successfully exploit a system vulnerability.

Vulnerability - Weaknesses in Smart Grid systems, cybersecurity procedures, internal controls, business processes, or implementations that could be exploited by a threat actor.

Acronyms

AMI - Advanced Metering Infrastructure

CIA -	Confidentiality, Integrity, and Availability. NISTIR 7628's Table 3-1 Impact Level Definitions (Vol. 1, Page 74) provides definitions for confidentiality, integrity, and availability, and identifies how they relate to potential impact levels.
CTR -	Common Technical Requirement
GRC -	Governance, Risk, and Compliance Requirement
LIC -	Logical Interface Category
NISTIR -	National Institute of Standards and Technology Interagency Report
NIST SP -	National Institute of Standards and Technology Special Publication
RMP -	Risk Management Process (in this document RMP refers to *Department of Energy Electricity Subsector Cybersecurity Risk Management Process*)
UTR -	Unique Technical Requirement

References

Department of Energy, Office of Electricity Delivery and Energy Reliability, DOE/OE-0003, *Electricity Subsector Cybersecurity Risk Management Process*, May 2012, http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp

Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, NIST, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

NISTIR 7628, *Guidelines for Smart Grid Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-level Requirements*, August 2010, SGIP Cyber Security Working Group, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

NISTIR 7628, *Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References*, August 2010, SGIP Cyber Security Working Group, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf.

NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, NIST Computer Security Division, Computer Security Resource Center, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms*, May 2013, NIST Computer Security Division, Computer Security Resource Center, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

CSWG-TC-001, *SGIP Guide for Assessing the High-level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cyber Security*, July 23, 2012, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGTesting.

NIST Smart Grid Collaboration Wiki, SGIP Site, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome.

Contributors

Thank you to the following members of the CSWG/SGCC NISTIR 7628 User's Guide Subgroup for their contributions in developing this document:

- Mark Ellison – Lead, DTE Energy
- Amanda Stallings, Public Utility Commission of Ohio
- Chuck Hunt, Wells Fargo
- Craig Rosen, Pacific Gas & Electric / FireEye
- Elizabeth Sisley, Calm Sunrise Consulting, LLC
- Irene Gassko, Florida Power & Light
- Jody Fraser, Pacific Gas & Electric
- Leonard Jacobs, Xcel Energy
- Leonard Tillman, Balch & Bingham LLP
- Marianne Swanson, NIST
- Neil Greenfield, American Electric Power, Inc.
- Scott Saunders, Sacramento Municipal Utility District
- Tanya Brewer, NIST
- Victoria Yan Pillitteri, NIST