

CHAPTER THREE

HIGH-LEVEL SECURITY REQUIREMENTS

This chapter includes the detailed descriptions for each of the security requirements. The analyses used to select and modify these security requirements are included in Appendix G. This chapter includes the following:

1. Determination of the confidentiality, integrity, and availability (CI&A) impact levels for each of the logical interface categories. (See [Table 3-2](#).)
2. The common governance, risk, and compliance (GRC), common technical, and unique technical requirements are allocated to the logical interface categories. Also, the impact levels are included for each requirement. (See [Table 3-3](#).)
3. The security requirements for the Smart Grid. Included are the detailed descriptions for each requirement.

This information is provided as guidance to organizations that are implementing, designing, and/or operating Smart Grid systems as a starting point for selecting and modifying security requirements. The information is to be used as a starting point only. Each organization will need to perform a risk analysis to determine the applicability of the following material.

3.1 CYBER SECURITY OBJECTIVES

For decades, power system operations have been managing the reliability of the power grid in which power *availability* has been the primary requirement, with information integrity as a secondary but increasingly critical requirement. Confidentiality of customer information is also important in the normal revenue billing processes and for privacy concerns. Although focused on accidental/inadvertent security problems, such as equipment failures, employee errors, and natural disasters, existing power system management technologies can be used and expanded to provide additional security measures.

Availability is the most important security objective for power system reliability. The time latency associated with availability can vary—

- ≤ 4 ms for protective relaying;
- Subseconds for transmission wide-area situational awareness monitoring;
- Seconds for substation and feeder SCADA data;
- Minutes for monitoring noncritical equipment and some market pricing information;
- Hours for meter reading and longer-term market pricing information; and
- Days/weeks/months for collecting long-term data such as power quality information.

Integrity for power system operations includes assurance that—

- Data has not been modified without authorization;
- Source of data is authenticated;

Victoria Pillitteri 1/3/13 1:04 PM

Deleted: Table 3-2

- Time stamp associated with the data is known and authenticated; and
- Quality of data is known and authenticated.

Confidentiality is the least critical for power system reliability. However, confidentiality is becoming more important, particularly with the increasing availability of customer information online—

- Privacy of customer information;
- Electric market information; and
- General corporate information, such as payroll, internal strategic planning, etc.

3.2 CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY IMPACT LEVELS

Following are the definitions for the security objectives of CI&A, as defined in statute.

Confidentiality

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

Integrity

“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” [44 U.S.C., Sec. 3542]

A loss of *integrity* is the unauthorized modification or destruction of information.

Availability

“Ensuring timely and reliable access to and use of information...” [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

Based on these definitions, impact levels for each security objective (confidentiality, integrity, and availability) are specified in [Table 3-1](#), as low, moderate, and high as defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. The impact levels are used in the selection of security requirements for each logical interface category.

Victoria Pillitteri 11/20/12 3:11 PM

Deleted: Table 3-1

Table 3-1 Impact Levels Definitions

	Potential Impact Levels		
	Low	Moderate	High
<p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

3.3 IMPACT LEVELS FOR THE CI&A CATEGORIES

Each of the three impact levels (i.e., low, moderate, high) is based upon the expected adverse effect of a security breach upon organizational operations, organizational assets, or individuals. The initial designation of impact levels focused on power grid reliability. The expected adverse effect on individuals when privacy breaches occur and adverse effects on financial markets when confidentiality is lost are included here for specific logical interface categories.

Power system reliability: Keep electricity flowing to customers, businesses, and industry. For decades, the power system industry has been developing extensive and sophisticated systems and equipment to avoid or shorten power system outages. In fact, power system operations have been termed the largest and most complex machine in the world. Although there are definitely new areas of cyber security concerns for power system reliability as technology opens new

opportunities and challenges, nonetheless, the existing energy management systems and equipment, possibly enhanced and expanded, should remain as key cyber security solutions.

Confidentiality and privacy of customers: As the Smart Grid reaches into homes and businesses, and as customers increasingly participate in managing their energy, confidentiality and privacy of their information has increasingly become a concern. Unlike power system reliability, customer privacy is a new issue.

The impact levels (low [L], moderate [M], and high [H]) presented in [Table 3-2](#), address the impacts to the nationwide power grid, particularly with regard to grid stability and reliability. Consequentially, the confidentiality impact is low for these logical interface categories. Logical interface categories 7, 8, 13, 14, 16, and 22 have a high impact level for confidentiality because of the type of data that needs to be protected (e.g., sensitive customer energy usage data, critical security parameters, and information from a HAN to a third party.)

Victoria Pillitteri 11/20/12 3:11 PM
Deleted: Table 3-2

Table 3-2 Smart Grid Impact Levels

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	H	H	L
19	L	H	M
20	L	H	M
21	L	H	L
22	H	H	H

Victoria Pillitteri 12/6/12 2:25 PM
Deleted: L

3.4 SELECTION OF SECURITY REQUIREMENTS

Power system operations pose many security challenges that are different from most other industries. In many cases, legacy equipment in industrial control systems that are in use in the power system operations may not be able to incorporate all requirements in this document, yet still need the protections offered by the requirements. For example, the Internet is different from the power system operations environment. In particular, there are strict performance and reliability requirements that are needed by power system operations. For instance—

- Operation of the power system must continue 24×7 with high availability (e.g., 99.99% for SCADA and higher for protective relaying) regardless of any compromise in security or the implementation of security measures that hinder normal or emergency power system operations.
- Power system operations must be able to continue during any security attack or compromise (as much as possible).
- Power system operations must recover quickly after a security attack or the compromise of an information system.
- Testing of security measures cannot be allowed to impact power system operations.
- Power system management, monitoring, and control will increasingly extend away from the power entities' traditional physical and security environments into external environments that the power entity has little or no influence and control over.

There is no single set of cyber security requirements that addresses each of the Smart Grid logical interface categories. This information can be used as guidelines for organizations as they develop their cyber security strategy, perform risk assessments, and select and modify security requirements for Smart Grid information system implementations.

Additional criteria must be used in determining the cyber security requirements before selecting and implementing the cyber security measures/solutions. These additional criteria must take into account the characteristics of the interface, including the constraints and issues posed by device and network technologies, the existence of legacy components/devices, varying organizational structures, regulatory and legal policies, and cost criteria.

Once these interface characteristics are applied, then cyber security requirements can be applied that are both specific enough to be applicable to the interfaces and general enough to permit the implementation of different cyber security solutions that meet the security requirements or embrace new security technologies as they are developed. This cyber security information can then be used in subsequent steps to select security requirements for the Smart Grid.

The security requirements listed below are an amalgam from several sources: NIST SP 800-53, the DHS Catalog, NERC CIPs, and the NRC Regulatory Guidance. After the security requirements were selected, they were modified as required. The goal was to develop a set of security requirements that address the needs of the electric sector and the Smart Grid. Each security requirement is allocated to one of three categories: governance, risk, and compliance (GRC), common technical, or unique technical. The intent of the GRC requirements is to have them addressed at the organization level. GRC requirements, while centered around policy, procedure, and compliance-based activities, may include technical implications. It may be necessary to augment these organization-level requirements for different types of organizational

Victoria Pillitteri 12/4/12 12:19 PM
Deleted: -

[security structures](#), specific logical interface categories and/or Smart Grid information systems. The common technical requirements are applicable to all of the logical interface categories. The unique technical requirements are allocated to one or more of the logical interface categories. The common and unique technical requirements should be allocated to each Smart Grid system and not necessarily to every component within a system, as the focus is on security at the system level. Each organization must develop a security architecture for each Smart Grid information system and allocate security requirements to components/devices. Some security requirements may be allocated to one or more components/devices. However, not every security requirement must be allocated to every component/device. Table 3-3 includes only the security requirements that were selected. There are additional security requirements included in the next section that were not selected. These may be included by an organization if it determines that the security requirements are necessary to address specific risks and needs.

For each unique technical requirement, the recommended security impact level is specified (e.g., low [L], moderate [M], or high [H]) in Table 3-3. The common technical requirements and GRC requirements apply to all logical interface categories. A recommended impact level is included with each of the common technical and GRC requirements. The requirement may be the same at all impact levels. If there are additional requirements at the moderate and high impact levels, these are listed in the table. The information included in the table is a guideline and presented as a starting point for organizations as they implement Smart Grid information systems. Each organization should use this guidance information as it implements the security strategy and performs the security risk assessment.

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

3.5 SECURITY REQUIREMENTS EXAMPLE

This example illustrates how to select security requirements using the material in this report. Included in this example are some GRC, common technical and unique technical requirements that may apply to a Smart Grid information system.

Example: Smart Grid control system “ABC” includes logical interface category 6: interface between control systems in different organizations. As specified in the previous chapter, this requires high data accuracy, high availability, and establishment of a chain of trust.

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

Victoria Pillitteri 12/3/12 2:59 PM

Comment [3]: Please link! ☺

SG.CM-6, Configuration Settings, the organization determines that there are unique settings for the ABC control system.

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

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

3.6 RECOMMENDED SECURITY REQUIREMENTS

Table 3-3 lists the selected GRC, common technical and unique technical security requirements and recommended impact level specifications for the logical interface categories for the Smart Grid. The security requirements that are not selected at any impact level are not shown in this table, but are included in the Sections 3.7 through 3.25. It is recommended that the GRC and common technical requirements be applied across all of the logical interfaces throughout the organization; while the unique technical requirements are only applied to select logical interfaces at select impact levels. When selecting impact levels of unique technical requirements to apply to specific logical interface categories, the CI&A requirements of both each logical interface category (see Table 3-2) and the unique technical requirement is considered. The final impact level allocation selection is not based on a high water-mark or formula that combines the CI&A categories, rather it reflects which of the CI&A tenants the unique technical requirement most strongly supports within the logical interface category. Hence, Table 3-3 identifies the recommended impact level allocation for each unique technical requirement as applied to each logical interface category to address its specific confidentiality, integrity, and availability needs.

The requirements and associated impact levels in this table provides only a summary of recommendations. For example, this table recommends that unique technical requirement SG.AC-12, Session Lock, is implemented for logical interfaces categories 7, 8, and 22 at a High impact level and logical interface categories 17 and 21 at a Low impact level. This does not mean that SG.AC-12 is only implemented if the impact level of the logical interface is High (or Low), cannot or should not be selected for other logical interface categories not listed in the table, or should be selected at an impact level that differs from the recommendation included in the table, if determined necessary as a result of the organization's risk assessment and risk tolerance. In either case, refer to the Impact Level Allocation section of the SG.AC-12 requirement to determine which impact levels the requirement could also be implemented for.

This table of recommendations is meant for use as a starting point for organizations. Each organization should conduct a risk assessment in accordance with their cyber security strategy to determine its risk tolerance and select the appropriate set of requirements to mitigate risk to an acceptable level.

Victoria Pillitteri 12/4/12 11:48 AM

Comment [4]: Waiting for feedback from MS on this text.

Table 3-3 Allocation of Security Requirements to Logical Interface Categories

Dark Gray = Unique Technical Requirement		Light Gray = Common Technical Requirement																				
White = Common Governance, Risk and Compliance (GRC)																						
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-11																						
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
SG.AC-16	Applies at all impact levels																					
SG.AC-17	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.AC-18	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
SG.AC-19	Applies at all impact levels																					
SG.AC-20	Applies at all impact levels																					
SG.AC-21	Applies at all impact levels																					

Victoria Pillitteri 12/4/12 11:49 AM
Formatted Table

Victoria Pillitteri 12/6/12 2:48 PM
Comment [5]: Check with a power systems person on this; perhaps not selected at any impact level.

Victoria Pillitteri 12/4/12 11:50 AM
Formatted Table

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.AT-1	Applies at all impact levels																						
SG.AT-2	Applies at all impact levels																						
SG.AT-3	Applies at all impact levels																						
SG.AT-4	Applies at all impact levels																						
SG.AT-6	Applies at all impact levels																						
SG.AT-7	Applies at all impact levels																						
SG.AU-1	Applies at all impact levels																						
SG.AU-2	Applies at all impact levels with additional requirement enhancements at high impact level																						
SG.AU-3	Applies at all impact levels																						
SG.AU-4	Applies at all impact levels																						
SG.AU-5	Applies at all impact levels with additional requirement enhancements at high impact level																						
SG.AU-6	Applies at all impact levels																						
SG.AU-7	Applies at moderate and high impact levels																						
SG.AU-8	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																						
SG.AU-9	Applies at all impact levels																						
SG.AU-10	Applies at all impact levels																						
SG.AU-11	Applies at all impact levels																						
SG.AU-12	Applies at all impact levels																						
SG.AU-13	Applies at all impact levels																						
SG.AU-14	Applies at all impact levels																						

Victoria Pillitteri 12/4/12 11:51 AM
Formatted Table

Victoria Pillitteri 12/4/12 11:52 AM
Formatted Table

Dark Gray = Unique Technical Requirement		Light Gray = Common Technical Requirement																					
White = Common Governance, Risk and Compliance (GRC)																							
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.AU-15	Applies at all impact levels																						
SG.AU-16							M	M	M					H	H		M				H	H	H
SG.CA-1	Applies at all impact levels																						
SG.CA-2	Applies at all impact levels																						
SG.CA-4	Applies at all impact levels																						
SG.CA-5	Applies at all impact levels																						
SG.CA-6	Applies at all impact levels																						
SG.CM-1	Applies at all impact levels																						
SG.CM-2	Applies at all impact levels																						
SG.CM-3	Applies at moderate and high impact levels																						
SG.CM-4	Applies at all impact levels																						
SG.CM-5	Applies at moderate and high impact levels																						
SG.CM-6	Applies at all impact levels																						
SG.CM-7	Applies at all impact levels																						
SG.CM-8	Applies at all impact levels																						
SG.CM-9	Applies at all impact levels																						
SG.CM-10	Applies at all impact levels																						
SG.CM-11	Applies at all impact levels																						

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.CP-1	Applies at all impact levels																																										
SG.CP-2	Applies at all impact levels																																										
SG.CP-3	Applies at all impact levels																																										
SG.CP-4	Applies at all impact levels																																										
SG.CP-5	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																																										
SG.CP-6	Applies at all impact levels																																										
SG.CP-7	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																																										
SG.CP-8	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																																										
SG.CP-9	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																																										
SG.CP-10	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																																										
SG.CP-11	Applies at high impact levels																																										
SG.IA-1	Applies at all impact levels																																										
SG.IA-2	Applies at all impact levels																																										
SG.IA-3	Applies at all impact levels																																										
SG.IA-4	H	H	H	H	H	H	M	M	M	H			H	H	M	M	H	H		H	H	H																					
SG.IA-5	H	H	H	H			M	M				M					H		H	H	H	H																					
SG.IA-6	L	L	L	L	L	L	H	H	L	L			H	H	L	H	L	L		L	L	H																					

Dark Gray = Unique Technical Requirement		Light Gray = Common Technical Requirement																					
White = Common Governance, Risk and Compliance (GRC)																							
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.ID-1	Applies at all impact levels																						
SG.ID-2	Applies at all impact levels																						
SG.ID-3	Applies at all impact levels																						
SG.ID-4	Applies at all impact levels																						
SG.IR-1	Applies at all impact levels																						
SG.IR-2	Applies at all impact levels																						
SG.IR-3	Applies at all impact levels																						
SG.IR-4	Applies at all impact levels																						
SG.IR-5	Applies at all impact levels																						
SG.IR-6	Applies at all impact levels																						
SG.IR-7	Applies at all impact levels																						
SG.IR-8	Applies at all impact levels																						
SG.IR-9	Applies at all impact levels																						
SG.IR-10	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																						
SG.IR-11	Applies at all impact levels																						
SG.MA-1	Applies at all impact levels																						
SG.MA-2	Applies at all impact levels																						
SG.MA-3	Applies at all impact levels with additional requirement enhancements at high impact levels																						
SG.MA-4	Applies at all impact levels																						

Dark Gray = Unique Technical Requirement		Light Gray = Common Technical Requirement																					
White = Common Governance, Risk and Compliance (GRC)																							
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.MA-5	Applies at all impact levels																						
SG.MA-6	Applies at all impact levels with additional requirement enhancements at high impact levels																						
SG.MA-7	Applies at all impact levels																						
SG.MP-1	Applies at all impact levels																						
SG.MP-2	Applies at all impact levels																						
SG.MP-3	Applies at moderate and high impact levels																						
SG.MP-4	Applies at all impact levels																						
SG.MP-5	Applies at all impact levels																						
SG.MP-6	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																						
SG.PE-1	Applies at all impact levels																						
SG.PE-2	Applies at all impact levels																						
SG.PE-3	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																						
SG.PE-4	Applies at all impact levels																						
SG.PE-5	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																						
SG.PE-6	Applies at all impact levels																						
SG.PE-7	Applies at all impact levels																						
SG.PE-8	Applies at all impact levels																						
SG.PE-9	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																						
SG.PE-10	Applies at all impact levels																						
SG.PE-11	Applies at all impact levels																						

Victoria Pillitteri 12/4/12 11:53 AM
Formatted Table

Dark Gray = Unique Technical Requirement		Light Gray = Common Technical Requirement																					
White = Common Governance, Risk and Compliance (GRC)																							
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.PE-12	Applies at all impact levels with additional requirement enhancements at high impact level																						
SG.PL-1	Applies at all impact levels																						
SG.PL-2	Applies at all impact levels																						
SG.PL-3	Applies at all impact levels																						
SG.PL-4	Applies at all impact levels																						
SG.PL-5	Applies at moderate and high impact levels																						
SG.PM-1	Applies at all impact levels																						
SG.PM-2	Applies at all impact levels																						
SG.PM-3	Applies at all impact levels																						
SG.PM-4	Applies at all impact levels																						
SG.PM-5	Applies at all impact levels																						
SG.PM-6	Applies at all impact levels																						
SG.PM-7	Applies at all impact levels																						
SG.PM-8	Applies at all impact levels																						
SG.PS-1	Applies at all impact levels																						
SG.PS-2	Applies at all impact levels																						
SG.PS-3	Applies at all impact levels																						
SG.PS-4	Applies at all impact levels																						
SG.PS-5	Applies at all impact levels																						

Victoria Pillitteri 12/4/12 11:53 AM
Deleted: all impact levels

Dark Gray = Unique Technical Requirement		Light Gray = Common Technical Requirement																					
White = Common Governance, Risk and Compliance (GRC)																							
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.PS-6	Applies at all impact levels																						
SG.PS-7	Applies at all impact levels																						
SG.PS-8	Applies at all impact levels																						
SG.PS-9	Applies at all impact levels																						
SG.RA-1	Applies at all impact levels																						
SG.RA-2	Applies at all impact levels																						
SG.RA-3	Applies at all impact levels																						
SG.RA-4	Applies at all impact levels																						
SG.RA-5	Applies at all impact levels																						
SG.RA-6	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																						
SG.SA-1	Applies at all impact levels																						
SG.SA-2	Applies at all impact levels																						
SG.SA-3	Applies at all impact levels																						
SG.SA-4	Applies at all impact levels																						
SG.SA-5	Applies at all impact levels																						
SG.SA-6	Applies at all impact levels																						
SG.SA-7	Applies at all impact levels																						
SG.SA-8	Applies at all impact levels																						
SG.SA-9	Applies at all impact levels																						
SG.SA-10	Applies at all impact levels																						

Victoria Pillitteri 12/4/12 11:54 AM
Formatted Table

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.SA-11	Applies at all impact levels																						
SG.SC-1	Applies at all impact levels																						
SG.SC-3	H	H	H	H			M	M					H	H	M	M		H		H	H	H	
SG.SC-5	H	M	H	M	M	M			M	M		M		H	M				M			H	
SG.SC-6					H									H								H	
SG.SC-7	H	H	H	H	H	H		M	M	H		M	H	H	M	M		H	H	H	H	H	
SG.SC-8	H	H	H	H	H	H	M	M	M	H	M	M	H	H	M	M		H	H	H	H	H	
SG.SC-9													H	H		H						H	
SG.SC-11	Applies at all impact levels with additional requirement enhancements at high impact levels																						
SG.SC-12	Applies at all impact levels																						
SG.SC-13	Applies at all impact levels																						
SG.SC-15	Applies at all impact levels																						
SG.SC-16	Applies at moderate and high impact levels																						
SG.SC-17	H	M	H	M	H	M			M	M	M	M		H	M		M		M	M		H	
SG.SC-18	Applies at all impact levels																						
SG.SC-19	Applies at all impact levels																						
SG.SC-20	Applies at all impact levels																						
SG.SC-21	Applies at all impact levels																						
SG.SC-22	Applies at moderate and high impact levels																						
SG.SC-26							H	H					H	H		H						H	

Victoria Pillitteri 12/4/12 11:56 AM
Comment [6]: Changed both SG.SA-10 and SG.SA-11 from Common Tech to GRC

Victoria Pillitteri 12/4/12 11:55 AM
Comment [7]: Remove SG.SC-6 (I couldn't delete a row from the table and have track changes show it)

Victoria Pillitteri 12/6/12 2:52 PM
Formatted: Centered

Victoria Pillitteri 12/4/12 11:56 AM
Formatted Table

Victoria Pillitteri 12/4/12 11:56 AM
Comment [8]: Changed from Common Tech to GRC

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement White = Common Governance, Risk and Compliance (GRC)																						
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.SC-29	H	H	H	H	H	H				H			H	H			H	H	H	H	H	H
SG.SC-30	Applies at moderate and high impact levels																					
SG.SI-1	Applies at all impact levels																					
SG.SI-2	Applies at all impact levels																					
SG.SI-3	Applies at all impact levels																					
SG.SI-4	Applies at all impact levels																					
SG.SI-5	Applies at all impact levels																					
SG.SI-6	Applies at moderate and high impact levels																					
SG.SI-7	H	H	H	H	H	H	M	M	M	H		M	H	H	M	M	H	H	H	H	H	H
SG.SI-8	Applies at moderate and high impact levels																					
SG.SI-9	Applies at all impact levels																					

Victoria Pillitteri 12/4/12 11:56 AM
Formatted Table

Victoria Pillitteri 12/4/12 11:57 AM
Comment [9]: SG.SI-2 and SG.SI-3 - Changed from GRC to Common Tech

3.6.1 Security Requirements

This section contains the recommended security requirements for the Smart Grid. The recommended security requirements are organized into families primarily based on NIST SP 800-53. A cross-reference of the Smart Grid security requirements to NIST SP 800-53, the DHS Catalog, and the NERC CIPs is included in Appendix A.

The following information is included with each security requirement:

1. Security requirement identifier and name. Each security requirement has a unique identifier that consists of three components. The initial component is SG – for Smart Grid. The second component is the family name, e.g., AC for access control and CP for Continuity of Operations. The third component is a unique numeric identifier, for example, SG.AC-1 and SG.CP-3. Each requirement also has a unique name.
2. Category. Identifies whether the security requirement is a GRC, common technical, or unique technical requirement. For each common technical security requirement, the most applicable objective (confidentiality, integrity, and availability) is listed.
3. The *Requirement* describes specific security-related activities or actions to be carried out by the organization or by the Smart Grid information system.
4. The *Supplemental Guidance* section provides additional information that may be useful in understanding the security requirement. This information is guidance and is not part of the security requirement.
5. The *Requirement Enhancements* provide statements of security capability to (i) build additional functionality in a requirement, and/or (ii) increase the strength of a requirement. In both cases, the requirement enhancements are used in a Smart Grid information system requiring greater protection due to the potential impact of loss based on the results of a risk assessment. Requirement enhancements are numbered sequentially within each requirement.
6. The *Additional Considerations* provide additional statements of security capability that may be used to enhance the associated security requirement. These are provided for organizations to consider as they implement Smart Grid information systems and are not intended as security requirements. Each additional consideration is number A1, A2, etc., to distinguish them from the security requirements and requirement enhancements.
7. The *Impact Level Allocation* identifies the security requirement and requirement enhancements, as applicable, at each impact level: low, moderate, and high. The impact levels for a specific Smart Grid information system will be determined by the organization in the risk assessment process.

Organizations should use the security requirements presented in the following sections as guidelines as they implement their cybersecurity strategy, perform risk assessments, and select and tailor security requirements for their Smart Grid information system implementations.

After performing a risk assessment, an organization should select the appropriate set of cybersecurity requirements applicable to the selected logical interface category. These security requirements, including GRCs, common technical and unique technical, could then be tailored to meet the specific risk criteria and Smart Grid information system functional and performance

Victoria Pillitteri 12/3/12 4:38 PM

Formatted: NumList

Victoria Pillitteri 12/3/12 4:38 PM

Deleted: -

requirements, technical characteristics, and security vulnerabilities. Not all security requirements are assigned to impact levels, as indicated by the phrase “Not Selected.” In those cases, the security requirements should be applied as appropriate.

After the selection of the initial set of security requirements, the selected requirements should be tailored to ensure they are appropriately modified and closely aligned to address the conditions for the Smart Grid information system. This tailoring process includes:

- Selecting the appropriate security requirements, including GRCs, common technical, and unique technical;
- Identifying aspects of the selected security requirements that would need modifications or clarifications to apply to the Smart Grid information system;
- Identifying security policy issues in the GRCs to ensure they are covered in the appropriate security policies in the organization;
- Identifying how the common technical and unique technical requirements are or would be address in the Smart Grid information system design and implementation;
- Identifying security gaps where compensating security requirements or measures are needed; ensuring the compensating security requirements or measures meet the security goals of the organization; and
- Specifying, as appropriate, which security requirements should be met for different stakeholders of the Smart Grid information system (vendors, implementers, operations, maintenance, users, etc.).

The term *information* is used to include data that is received and data that is sent—including, for example, data that is interpreted as a command, a setting, or a request to send data.

The requirements related to emergency lighting, fire protection, temperature and humidity controls, water damage, power equipment and power cabling, and lockout/tagout²¹ are important requirements for safety. These are outside the scope of cyber security and are not included in this report. However, these requirements must be addressed by each organization in accordance with local, state, federal, and organizational regulations, policies, and procedures.

The requirements related to privacy are not included in this chapter. They are included in Chapter 5 of this report. Specifically, privacy principle recommendations based on the PIA are included in §5.4.2, Summary PIA Findings and Recommendations, and in §5.8, Smart Grid Privacy Summary and Recommendations.

3.7 ACCESS CONTROL (SG.AC)

The focus of access control is ensuring that resources are accessed only by the appropriate personnel, and that personnel are correctly identified. Mechanisms need to be in place to monitor access activities for inappropriate activity.

²¹ Lockout/tagout is a safety procedure which is used in industry to ensure that dangerous machines are properly shut off and not started up again prior to the completion of maintenance or servicing work.

SG.AC-1 Access Control Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented access control security policy that addresses—
 - i. The objectives, roles, and responsibilities for the access control security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the access control security program as it applies to all of the organizational staff, contractors, and third parties.
 - b. Procedures to address the implementation of the access control security policy and associated access control protection requirements.
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
3. The organization ensures that the access control security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-1	Moderate: SG.AC-1	High: SG.AC-1
--------------	-------------------	---------------

SG.AC-2 Remote Access Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Documents allowed methods of remote access to the Smart Grid information system;
2. Establishes usage restrictions and implementation guidance for each allowed remote access method;
3. Authorizes remote access to the Smart Grid information system prior to connection; and
4. Enforces requirements for remote connections to the Smart Grid information system.

Victoria Pillitteri 12/4/12 12:04 PM

Comment [10]: Overall editorial – the font of numbers (across all HLR) is a different style (font style, indent level, bolded, size, etc.) than the rest of the numbering of the document.

Supplemental Guidance

Remote access is any access to an organizational Smart Grid information system by a user (or process acting on behalf of a user) communicating through an external, non-organization-controlled network (e.g., the Internet).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-2	Moderate: SG.AC-2	High: SG.AC-2
--------------	-------------------	---------------

SG.AC-3 Account Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization manages Smart Grid information system accounts, including:

1. Authorizing, establishing, activating, modifying, disabling, and removing accounts;
2. Specifying account types, access rights, and privileges (e.g., individual, group, system, guest, anonymous and temporary);
3. Reviewing accounts on an organization-defined frequency;
4. Notifying account managers when Smart Grid information system users are terminated, transferred, or Smart Grid information system usage changes; and
5. Requiring management approval prior to establishing accounts.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization reviews currently active Smart Grid information system accounts on an organization-defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy.
- A2. The organization authorizes and monitors the use of guest/anonymous accounts.
- A3. The organization employs automated mechanisms to support the management of Smart Grid information system accounts.
- A4. The Smart Grid information system automatically terminates temporary and emergency accounts after an organization-defined time period for each type of account.

Victoria Pillitteri 12/4/12 12:02 PM
Comment [11]: Reformatted numbering in this requirement, reworded last part of requirement to fit list sentence structure.

Victoria Pillitteri 12/4/12 12:00 PM
Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Victoria Pillitteri 12/4/12 12:01 PM
Deleted: and

Victoria Pillitteri 12/4/12 12:01 PM
Deleted: .

Victoria Pillitteri 12/4/12 12:01 PM
Formatted: NumList

Victoria Pillitteri 12/4/12 12:01 PM
Deleted: M

Victoria Pillitteri 12/4/12 12:01 PM
Deleted: is required

- A5. The Smart Grid information system automatically disables inactive accounts after an organization-defined time period.
- A6. The Smart Grid information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.

Impact Level Allocation

Low: SG.AC-3	Moderate: SG.AC-3	High: SG.AC-3
--------------	-------------------	---------------

SG.AC-4 Access Enforcement

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system enforces assigned authorizations for controlling access to the Smart Grid information system in accordance with organization-defined policy.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization considers the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies.

Impact Level Allocation

Low: SG.AC-4	Moderate: SG.AC-4	High: SG.AC-4
--------------	-------------------	---------------

SG.AC-5 Information Flow Enforcement

Category: Unique Technical Requirements

Requirement

The Smart Grid information system enforces assigned authorizations for controlling the flow of information within the Smart Grid information system and between interconnected Smart Grid information systems in accordance with applicable policy.

Supplemental Guidance

Information flow control regulates where information is allowed to travel within a Smart Grid information system and between Smart Grid information systems. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict Smart Grid information system services or provide a packet-filtering capability.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system enforces information flow control using explicit labels on information, source, and destination objects as a basis for flow control decisions.
- A2. The Smart Grid information system enforces dynamic information flow control allowing or disallowing information flows based on changing conditions or operational considerations.
- A3. The Smart Grid information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions.
- A4. The Smart Grid information system enforces the use of human review for organization-defined security policy filters when the Smart Grid information system is not capable of making an information flow control decision.
- A5. The Smart Grid information system provides the capability for a privileged administrator to configure, enable, and disable the organization-defined security policy filters.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.AC-6 Separation of Duties

Category: Common Technical Requirements, Integrity

Requirement

The organization—

- 1. Establishes and documents divisions of responsibility and separates functions as needed to eliminate conflicts of interest and to ensure independence in the responsibilities and functions of individuals/roles;
- 2. Enforces separation of Smart Grid information system functions through assigned access authorizations; and
- 3. Restricts security functions to the least amount of users necessary to ensure the security of the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-6	High: SG.AC-6
-------------------	-------------------	---------------

SG.AC-7 Least Privilege

Category: Common Technical Requirements, Integrity

Requirement

The organization -

1. Assigns the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks; and
2. Configures the Smart Grid information system to enforce the most restrictive set of rights and privileges or access needed by users.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization authorizes network access to organization-defined privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system.
- A2. The organization authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-7	High: SG.AC-7
-------------------	-------------------	---------------

SG.AC-8 Unsuccessful Login Attempts

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period.

Supplemental Guidance

Because of the potential for denial of service, automatic lockouts initiated by the Smart Grid information system are usually temporary and automatically released after a predetermined time period established by the organization. Permanent automatic lockouts initiated by a Smart Grid information system must be carefully considered before being used because of safety considerations and the potential for denial of service.

Requirement Enhancements

None.

Additional Considerations

Victoria Pillitteri 12/4/12 12:03 PM

Deleted: The organization a

Victoria Pillitteri 12/4/12 12:03 PM

Deleted: The organization c

- A1. The Smart Grid information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded; and
- A2. If a Smart Grid information system cannot perform account/node locking or delayed logins because of significant adverse impact on performance, safety, or reliability, the system employs alternative requirements or countermeasures that include the following:
 - a. Real-time logging and recording of unsuccessful login attempts; and
 - b. Real-time alerting of a management authority for the Smart Grid information system when the number of defined consecutive invalid access attempts is exceeded.

Impact Level Allocation

Low: SG.AC-8	Moderate: SG.AC-8	High: SG.AC-8
--------------	-------------------	---------------

SG.AC-9 Smart Grid Information System Use Notification

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system displays an approved system use notification message or banner before granting access to the Smart Grid information system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance.

Supplemental Guidance

Smart Grid information system use notification messages can be implemented in the form of warning banners displayed when individuals log in to the Smart Grid information system. Smart Grid information system use notification is intended only for Smart Grid information system access that includes an interactive interface with a human user and is not intended to call for such an interface when the interface does not currently exist.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-9	Moderate: SG.AC-9	High: SG.AC-9
--------------	-------------------	---------------

SG.AC-10 Previous Logon Notification

Category: Unique Technical Requirements

Requirement

The Smart Grid information system notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.AC-11 Concurrent Session Control

Category: Unique Technical Requirements, [Availability](#)

Requirement

The organization limits the number of concurrent sessions for any user on the Smart Grid information system.

Supplemental Guidance

The organization may define the maximum number of concurrent sessions for a Smart Grid information system account globally, by account type, by account, or a combination. This requirement addresses concurrent sessions for a given Smart Grid information system account and does not address concurrent sessions by a single user via multiple Smart Grid information system accounts.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-11	High: SG.AC-11
-------------------	--------------------	----------------

SG.AC-12 Session Lock

Category: Unique Technical Requirements

Requirement

The Smart Grid information system—

1. Prevents further access to the Smart Grid information system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance

Victoria Pillitteri 12/6/12 2:45 PM
Comment [12]: Need to talk to power system engr about this regarding:
Should it apply to any of the LICs?
What impact levels this should apply?

A session lock is not a substitute for logging out of the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-12	High: SG.AC-12
-------------------	--------------------	----------------

SG.AC-13 Remote Session Termination

Category: Unique Technical Requirements

Requirement

The Smart Grid information system terminates a remote session at the end of the session or after an organization-defined time period of inactivity.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. Automatic session termination applies to local and remote sessions.

Impact Level Allocation

Low: Not Selected	Moderate: SG.AC-13	High: SG.AC-13
-------------------	--------------------	----------------

SG.AC-14 Permitted Actions without Identification or Authentication

Category: Unique Technical Requirements

Requirement

The organization -

1. Identifies and documents specific user actions, if any, that can be performed on the Smart Grid information system without identification or authentication; and
2. Identifies 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

Victoria Pillitteri 12/4/12 12:05 PM
Deleted: The organization i

Victoria Pillitteri 12/4/12 12:05 PM
Deleted: Organizations identify

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)
---------------	------------------------	--------------------

SG.AC-15 Remote Access

Category: Unique Technical Requirements

Requirement

The organization authorizes, monitors, and manages all methods of remote access to the Smart Grid information system.

Supplemental Guidance

Remote access is any access to a Smart Grid information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Requirement Enhancements

1. The organization authenticates remote access, and uses cryptography to protect the confidentiality and integrity of remote access sessions;
2. The Smart Grid information system routes all remote accesses through a limited number of managed access control points;
3. The Smart Grid information system protects wireless access to the Smart Grid information system using authentication and encryption. Note: Authentication applies to user, device, or both as necessary; and
4. The organization monitors for unauthorized remote connections to the Smart Grid information system, including scanning for unauthorized wireless access points on an organization-defined frequency and takes appropriate action if an unauthorized connection is discovered.

Additional Considerations

- A1. Remote access to Smart Grid information system component locations (e.g., control center, field locations) is enabled only when necessary, approved, authenticated, and for the duration necessary;
- A2. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods;

- A3. The organization authorizes remote access for privileged commands and security-relevant information only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system; and
- A4. The organization disables, when not intended for use, wireless networking capabilities internally embedded within Smart Grid information system components.

Impact Level Allocation

Low: SG.AC-15	Moderate: SG.AC-15 (1), (2), (3), (4)	High: SG.AC-15 (1), (2), (3), (4)
---------------	---------------------------------------	-----------------------------------

SG.AC-16 Wireless Access Restrictions

Category: Common Technical Requirements, Confidentiality

Requirement

The organization—

- 1. Establishes use restrictions and implementation guidance for wireless technologies; and
- 2. Authorizes, monitors, and manages wireless access to the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization uses authentication and encryption to protect wireless access to the Smart Grid information system; and
- A2. The organization scans for unauthorized wireless access points at an organization-defined frequency and takes appropriate action if such access points are discovered.

Impact Level Allocation

Low: SG.AC-16	Moderate: SG.AC-16	High: SG.AC-16
---------------	--------------------	----------------

SG.AC-17 Access Control for Portable and Mobile Devices

Category: Common Technical Requirements, Confidentiality

Requirement

The organization—

- 1. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices, including the use of writeable, removable media and personally owned removable media;
- 2. Authorizes connection of mobile devices to Smart Grid information systems;
- 3. Monitors for unauthorized connections of mobile devices to Smart Grid information systems; and

- Enforces requirements for the connection of mobile devices to Smart Grid information systems.

Supplemental Guidance

Specially configured mobile devices include computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel to locations that the organization determines to be of significant risk, include examining the device for signs of physical tampering and purging/reimaging the hard disk drive.

Requirement Enhancements

The organization—

- Controls the use of writable, removable media in Smart Grid information systems;
- Controls the use of personally owned, removable media in Smart Grid information systems;
- Issues specially configured mobile devices to individuals traveling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; and
- Applies specified measures to mobile devices returning from locations that the organization determines to be of significant risk in accordance with organizational policies and procedures.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-17	Moderate: SG.AC-17 (1), (2)	High: SG.AC-17 (1), (2), (3), (4)
---------------	-----------------------------	-----------------------------------

SG.AC-18 Use of External Information Control Systems

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes terms and conditions for authorized individuals to—

- Access the Smart Grid information system from an external information system; and
- Process, store, and transmit organization-controlled information using an external information system.

Supplemental Guidance

External information systems are information systems or components of information systems that are outside the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of security requirements or the assessment of security requirement effectiveness.

Requirement Enhancements

1. The organization imposes restrictions on authorized individuals with regard to the use of organization-controlled removable media on external information systems.

Additional Considerations

A1. The organization prohibits authorized individuals from using an external information system to access the Smart Grid information system or to process, store, or transmit organization-controlled information except in situations where the organization (a) can verify the implementation of required security controls on the external information system as specified in the organization’s security policy and security plan, or (b) has approved Smart Grid information system connection or processing agreements with the organizational entity hosting the external information system.

Impact Level Allocation

Low: SG.AC-18	Moderate: SG.AC-18 (1)	High: SG.AC-18 (1)
---------------	------------------------	--------------------

SG.AC-19 Control System Access Restrictions

Category: Common Technical Requirements

Requirement

The organization employs mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization’s enterprise network.

Supplemental Guidance

Access to the Smart Grid information system to satisfy business requirements needs to be limited to read-only access.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-19	Moderate: SG.AC-19	High: SG.AC-19
---------------	--------------------	----------------

SG.AC-20 Publicly Accessible Content

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Designates individuals authorized to post information onto an organizational information system that is publicly accessible;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

Victoria Pillitteri 12/4/12 12:05 PM
Deleted: Common Governance, Risk, and Compliance (GRC)

3. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;
4. Reviews the content on the publicly accessible organizational information system for nonpublic information on an organization-defined frequency; and
5. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

Supplemental Guidance

Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This requirement addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-20	Moderate: SG.AC-20	High: SG.AC-20
---------------	--------------------	----------------

SG.AC-21 Passwords

Category: Common Technical Requirements, Integrity

Requirement

1. The organization develops and enforces policies and procedures for Smart Grid information system users concerning the generation and use of passwords;
2. These policies stipulate rules of complexity, based on the criticality level of the Smart Grid information system to be accessed; and
3. Passwords shall be changed regularly and are revoked after an extended period of inactivity.

Supplemental Guidance

[NIST Special Publication 800-63, Electronic Authentication Guideline, Appendix A, provides additional guidance on passwords.](#)

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AC-21	Moderate: SG.AC-21	High: SG.AC-21
---------------	--------------------	----------------

Victoria Pillitteri 12/4/12 12:06 PM
Deleted: None.

3.8 AWARENESS AND TRAINING (SG.AT)

Smart Grid information system security awareness is a critical part of Smart Grid information system incident prevention. Implementing a Smart Grid information system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals' roles and responsibilities.

SG.AT-1 Awareness and Training Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented awareness and training security policy that addresses—
 - i. The objectives, roles, and responsibilities for the awareness and training security program as it relates to protecting the organization's personnel and assets, and
 - ii. The scope of the awareness and training security program as it applies to all of the organizational staff, contractors, and third parties.
 - b. Procedures to address the implementation of the awareness and training security policy and associated awareness and training protection requirements.
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the awareness and training security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-1	Moderate: SG.AT-1	High: SG.AT-1
--------------	-------------------	---------------

SG.AT-2 Security Awareness

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides basic security awareness briefings to all Smart Grid information system users (including employees, contractors, and third parties) on an organization-defined frequency.

Supplemental Guidance

The organization determines the content of security awareness briefings based on the specific requirements of the organization and the Smart Grid information system to which personnel have authorized access.

Requirement Enhancements

None.

Additional Considerations

- A1. All Smart Grid information system design and procedure changes need to be reviewed by the organization for inclusion in the organization security awareness training; and
- A2. The organization includes practical exercises in security awareness briefings that simulate actual cyber attacks.

Impact Level Allocation

Low: SG.AT-2	Moderate: SG.AT-2	High: SG.AT-2
--------------	-------------------	---------------

SG.AT-3 Security Training

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides security-related training—

- 1. Before authorizing access to the Smart Grid information system or performing assigned duties;
- 2. When required by Smart Grid information system changes; and
- 3. On an organization-defined frequency thereafter.

Supplemental Guidance

The organization determines the content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the Smart Grid information system to which personnel have authorized access. In addition, the organization provides Smart Grid information system managers, Smart Grid information system and network administrators, and other personnel having access to Smart Grid information system-level software, security-related training to perform their assigned duties.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-3	Moderate: SG.AT-3	High: SG.AT-3
--------------	-------------------	---------------

SG.AT-4 Security Awareness and Training Records

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization maintains a record of awareness and training for each user in accordance with the provisions of the organization’s training and records retention policy.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-4	Moderate: SG.AT-4	High: SG.AT-4
--------------	-------------------	---------------

SG.AT-5 Contact with Security Groups and Associations

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes and maintains contact with security groups and associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance

Security groups and associations can include special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization’s mission/business requirements.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.AT-6 Security Responsibility Testing

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization -

1. Tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the Smart Grid information system;
2. Maintains a list of security responsibilities for roles that are used to test each user in accordance with the provisions of the organization training policy; and
3. Ensures security responsibility is conducted on an organization-defined frequency and as warranted by technology/procedural changes.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-6	Moderate: SG.AT-6	High: SG.AT-6
--------------	-------------------	---------------

SG.AT-7 Planning Process Training

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization includes training in its planning process on the implementation of the Smart Grid information system security plans for employees, contractors, and third parties.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AT-7	Moderate: SG. AT-7	High: SG. AT-7
--------------	--------------------	----------------

Victoria Pillitteri 12/4/12 12:09 PM

Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 12:09 PM

Deleted: he organization t

Victoria Pillitteri 12/4/12 12:09 PM

Deleted: The organization m

Victoria Pillitteri 12/4/12 12:10 PM

Deleted: The

Victoria Pillitteri 12/4/12 12:10 PM

Deleted: testing needs to be

Victoria Pillitteri 12/4/12 12:10 PM

Deleted: the organization's

3.9 AUDIT AND ACCOUNTABILITY (SG.AU)

Periodic audits and logging of the Smart Grid information system need to be implemented to validate that the security mechanisms present during Smart Grid information system validation testing are still installed and operating correctly. These security audits review and examine a

Smart Grid information system’s records and activities to determine the adequacy of Smart Grid information system security requirements and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of Smart Grid information system logs. Logging is necessary for anomaly detection as well as forensic analysis. With the convergence of power systems and traditional IT systems, proper analysis of event information is necessary in order to understand what occurred during the event. This analysis must acknowledge both disciplines, organizations will benefit from joint analysis of events. For example, analysis teams need to evaluate power systems logging data and cyber event logs in order to properly ascertain the actual causes of an event.

SG.AU-1 Audit and Accountability Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented audit and accountability security policy that addresses—
 - i. The objectives, roles, and responsibilities for the audit and accountability security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the audit and accountability security program as it applies to all of the organizational staff, contractors, and third parties.
 - b. Procedures to address the implementation of the audit and accountability security policy and associated audit and accountability protection requirements.
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
3. The organization ensures that the audit and accountability security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The audit and accountability policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-1	Moderate: SG.AU-1	High: SG.AU-1
--------------	-------------------	---------------

SG.AU-2 Auditable Events

Category: Common Technical Requirements, Integrity

Requirement

The organization—

1. Develops, based on a risk assessment, the Smart Grid information system list of auditable events on an organization-defined frequency;
2. Includes execution of privileged functions in the list of events to be audited by the Smart Grid information system; and
3. Revises the list of auditable events based on current threat data, assessment of risk, and post-incident analysis.

Supplemental Guidance

The purpose of this requirement is for the organization to identify events that need to be auditable as significant and relevant to the security of the Smart Grid information system.

Requirement Enhancements

1. The organization should audit activities associated with configuration changes to the Smart Grid information system.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-2	Moderate: SG.AU-2 (1)	High: SG.AU-2 (1)
--------------	-----------------------	-------------------

SG.AU-3 Content of Audit Records

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system produces audit records for each event. The record contains the following information:

- Data and time of the event,
- The component of the Smart Grid information system where the event occurred,
- Type of event,
- User/subject identity, and
- The outcome of the events.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject; and
- A2. The Smart Grid information system provides the capability to centrally manage the content of audit records generated by individual components throughout the Smart Grid information system.

Impact Level Allocation

Low: SG.AU-3	Moderate: SG.AU-3	High: SG.AU-3
--------------	-------------------	---------------

SG.AU-4 Audit Storage Capacity

Category: Common Technical Requirements, Integrity

Requirement

The organization allocates organization-defined audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance

The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-4	Moderate: SG.AU-4	High: SG.AU-4
--------------	-------------------	---------------

SG.AU-5 Response to Audit Processing Failures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system—

1. Alerts designated organizational officials in the event of an audit processing failure; and
2. Executes an organization-defined set of actions to be taken (e.g., shutdown Smart Grid information system, overwrite oldest audit records, and stop generating audit records).

Supplemental Guidance

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Requirement Enhancements

1. The Smart Grid information system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity; and
2. The Smart Grid information system provides a real-time alert for organization defined audit failure events.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-5	Moderate: SG.AU-5	High: SG.AU-5 (1), (2)
--------------	-------------------	------------------------

SG.AU-6 Audit Monitoring, Analysis, and Reporting

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Reviews and analyzes Smart Grid information system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to management authority; and
2. Adjusts the level of audit review, analysis, and reporting within the Smart Grid information system when a change in risk occurs to organizational operations, organizational assets, or individuals.

Supplemental Guidance

Organizations increase the level of audit monitoring and analysis activity within the Smart Grid information system based on, for example, law enforcement information, intelligence information, or other credible sources of information.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities;
- A2. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness;
- A3. The Smart Grid information system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the Smart Grid information system; and
- A4. The organization integrates analysis of audit records with analysis of performance and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

Impact Level Allocation

Low: SG.AU-6	Moderate: SG.AU-6	High: SG.AU-6
--------------	-------------------	---------------

SG.AU-7 Audit Reduction and Report Generation

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system provides an audit reduction and report generation capability.

Supplemental Guidance

Audit reduction and reporting may support near real-time analysis and after-the-fact investigations of security incidents.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system provides the capability to automatically process audit records for events of interest based on selectable event criteria

Impact Level Allocation

Low: Not Selected	Moderate: SG.AU-7	High: SG.AU-7
-------------------	-------------------	---------------

SG.AU-8 Time Stamps

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance

Time stamps generated by the information system include both date and time, as defined by the organization.

Requirement Enhancements

1. The Smart Grid information system synchronizes internal Smart Grid information system clocks on an organization-defined frequency using an organization-defined, accurate, time source.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-8	Moderate: SG.AU-8 (1)	High: SG.AU-8 (1)
--------------	-----------------------	-------------------

SG.AU-9 Protection of Audit Information

Category: Common Technical Requirements

Requirement

The Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance

Audit information includes, for example, audit records, audit settings, and audit reports.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system produces audit records on hardware-enforced, write-once media.

Impact Level Allocation

Low: SG.AU-9	Moderate: SG.AU-9	High: SG.AU-9
--------------	-------------------	---------------

SG.AU-10 Audit Record Retention

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization retains audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-10	Moderate: SG.AU-10	High: SG.AU-10
---------------	--------------------	----------------

SG.AU-11 Conduct and Frequency of Audits

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization conducts audits on an organization-defined frequency to assess conformance to specified security requirements and applicable laws and regulations.

Victoria Pillitteri 12/4/12 12:45 PM

Deleted: Governance, Risk, and Compliance (GRC)

Supplemental Guidance

Audits can be either in the form of internal self-assessment (sometimes called first-party audits) or independent, third-party audits.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-11	Moderate: SG.AU-11	High: SG.AU-11
---------------	--------------------	----------------

SG.AU-12 Auditor Qualification

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization's audit program specifies auditor qualifications.

Supplemental Guidance

Security auditors need to—

1. Understand the Smart Grid information system and the associated operating practices;
2. Understand the risk involved with the audit; and
3. Understand the organization cyber security and the Smart Grid information system policy and procedures.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization assigns auditor and Smart Grid information system administration functions to separate personnel.

Impact Level Allocation

Low: SG.AU-12	Moderate: SG.AU-12	High: SG.AU-12
---------------	--------------------	----------------

SG.AU-13 Audit Tools

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization specifies the rules and conditions of use of audit tools.

Supplemental Guidance

Access to Smart Grid information systems audit tools needs to be protected to prevent any possible misuse or compromise.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-13	Moderate: SG.AU-13	High: SG.AU-13
---------------	--------------------	----------------

SG.AU-14 Security Policy Compliance

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program.

Supplemental Guidance

Periodic audits of the Smart Grid information system are implemented to demonstrate compliance to the organization's security policy. These audits—

1. Assess whether the defined cyber security policies and procedures, including those to identify security incidents, are being implemented and followed;
2. Document and ensure compliance to organization policies and procedures;
3. Identify security concerns, validate that the Smart Grid information system is free from security compromises, and provide information on the nature and extent of compromises should they occur;
4. Validate change management procedures and ensure that they produce an audit trail of reviews and approvals of all changes;
5. Verify that security mechanisms and management practices present during Smart Grid information system validation are still in place and functioning;
6. Ensure reliability and availability of the Smart Grid information system to support safe operation; and
7. Continuously improve performance.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.AU-14	Moderate: SG.AU-14	High: SG.AU-14
---------------	--------------------	----------------

SG.AU-15 Audit Record Generation

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system—

1. Provides audit record generation capability and generates audit records for the selected list of auditable events; and
2. Provides audit record generation capability and allows authorized users to select auditable events at the organization-defined Smart Grid information system components.

Supplemental Guidance

Audit records can be generated from various components within the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system provides the capability to consolidate audit records from multiple components within the Smart Grid information system into a Smart Grid information system-wide audit trail that is time-correlated to within an organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.

Impact Level Allocation

Low: SG.AU-15	Moderate: SG.AU-15	High: SG.AU-15
---------------	--------------------	----------------

SG.AU-16 Non-Repudiation

Category: Unique Technical Requirements

Requirement

The Smart Grid information system protects against an individual falsely denying having performed a particular action.

Supplemental Guidance

Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services are implemented using various techniques (e.g., digital signatures, digital message receipts, and logging).

Requirement Enhancements

None.

Additional Considerations

None.

Victoria Pillitteri 12/4/12 12:46 PM

Deleted: compile

Impact Level Allocation

Low: Not Selected	Moderate: SG.AU-16	High: SG.AU-16
-------------------	-------------------------------	----------------

Victoria Pillitteri 12/4/12 12:47 PM

Deleted: Not Selected

3.10 SECURITY ASSESSMENT AND AUTHORIZATION (SG.CA)

Security assessments include monitoring and reviewing the performance of Smart Grid information system. Internal checking methods, such as compliance audits and incident investigations, allow the organization to determine the effectiveness of the security program. Finally, through continuous monitoring, the organization regularly reviews compliance of the Smart Grid information systems. If deviations or nonconformance exist, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.

SG.CA-1 Security Assessment and Authorization Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented security assessment and authorization policy that addresses—
 - i. The objectives, roles, and responsibilities for the security assessment and authorization security program as it relates to protecting the organization's personnel and assets; and
 - ii. The scope of the security assessment and authorization security program as it applies to all of the organizational staff and third-party contractors; and
 - b. Procedures to address the implementation of the security assessment and authorization policy and associated security assessment and authorization protection requirements;
2. Management commitment ensures compliance with the organization's security assessment and authorization security policy and other regulatory requirements; and
3. The organization ensures that the security assessment and authorization security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The authorization to operate and security assessment policies can be included as part of the general information security policy for the organization. Authorization to operate and security assessment procedures can be developed for the security program in general and for a particular Smart Grid information system when required. The organization defines significant change to a Smart Grid information system for security reauthorizations.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CA-1	Moderate: SG.CA-1	High: SG.CA-1
--------------	-------------------	---------------

SG.CA-2 Security Assessments

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Develops a security assessment plan that describes the scope of the assessment including—
 - a. Security requirements and requirement enhancements under assessment;
 - b. Assessment procedures to be used to determine security requirement effectiveness; and
 - c. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security requirements assessment to a management authority.

Supplemental Guidance

The organization assesses the security requirements in a Smart Grid information system as part of authorization or reauthorization to operate and continuous monitoring. Previous security assessment results may be reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs an independent assessor or assessment team to conduct an assessment of the security requirements in the Smart Grid information system.

Impact Level Allocation

Low: SG.CA-2	Moderate: SG.CA-2	High: SG.CA-2
--------------	-------------------	---------------

SG.CA-3 Continuous Improvement

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization’s security program implements continuous improvement practices to ensure that industry lessons learned and best practices are incorporated into Smart Grid information system security policies and procedures.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.CA-4 Smart Grid Information System Connections

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Authorizes all connections from the Smart Grid information system to other information systems;
2. Documents the Smart Grid information system connections and associated security requirements for each connection; and
3. Monitors the Smart Grid information system connections on an ongoing basis, verifying enforcement of documented security requirements.

Supplemental Guidance

The organization considers the risk that may be introduced when a Smart Grid information system is connected to other information systems, both internal and external to the organization, with different security requirements. Risk considerations also include Smart Grid information systems sharing the same networks.

Requirement Enhancements

None.

Additional Considerations

- A1. All external Smart Grid information system and communication connections are identified and protected from tampering or damage.

Impact Level Allocation

Low: SG.CA-4	Moderate: SG.CA-4	High: SG.CA-4
--------------	-------------------	---------------

SG.CA-5 Security Authorization to Operate

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization authorizes the Smart Grid information system for processing before operation and updates the authorization based on an organization-defined frequency or when a significant change occurs to the Smart Grid information system; and
2. A management authority signs and approves the security authorization to operate. Security assessments conducted in support of security authorizations need to be reviewed on an organization-defined frequency.

Supplemental Guidance

The organization assesses the security mechanisms implemented within the Smart Grid information system prior to security authorization to operate.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CA-5	Moderate: SG.CA-5	High: SG.CA-5
--------------	-------------------	---------------

SG.CA-6 Continuous Monitoring

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy; and
2. Reporting the security state of the Smart Grid information system to management authority on an organization-defined frequency.

Supplemental Guidance

A continuous monitoring program allows an organization to maintain the security authorization to operate of a Smart Grid information system over time in a dynamic operational environment with changing threats, vulnerabilities, technologies, and missions/business processes.

The selection of an appropriate subset of security requirements for continuous monitoring is based on the impact level of the Smart Grid information system, the specific security requirements selected by the organization, and the level of assurance that the organization requires.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs an independent assessor or assessment team to monitor the security requirements in the Smart Grid information system on an ongoing basis;
- A2. The organization includes as part of security requirements continuous monitoring, periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises; and
- A3. The organization uses automated support tools for continuous monitoring.

Impact Level Allocation

Low: SG.CA-6	Moderate: SG.CA-6	High: SG.CA-6
--------------	-------------------	---------------

3.11 CONFIGURATION MANAGEMENT (SG.CM)

The organization’s security program needs to implement policies and procedures that create a process by which the organization manages and documents all configuration changes to the Smart Grid information system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the Smart Grid information system configuration. Smart Grid information systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a Smart Grid information system. Vendor updates and patches need to be thoroughly tested on a non-production Smart Grid information system setup before being introduced into the production environment to ensure that no adverse effects occur.

SG.CM-1 Configuration Management Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

- 1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented configuration management security policy that addresses—
 - i. The objectives, roles, and responsibilities for the configuration management security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the configuration management security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the configuration management security policy and associated configuration management protection requirements;
- 2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and

3. The organization ensures that the configuration management security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The configuration management policy can be included as part of the general system security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-1	Moderate: SG.CM-1	High: SG.CM-1
--------------	-------------------	---------------

SG.CM-2 Baseline Configuration

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops, documents, and maintains a current baseline configuration of the Smart Grid information system and an inventory of the Smart Grid information system's constituent components. The organization reviews and updates the baseline configuration as an integral part of Smart Grid information system component installations.

Supplemental Guidance

Maintaining the baseline configuration involves updating the baseline as the Smart Grid information system changes over time and keeping previous baselines for possible rollback.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration; and
- A2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the Smart Grid information system.

Impact Level Allocation

Low: SG.CM-2	Moderate: SG.CM-2	High: SG.CM-2
--------------	-------------------	---------------

SG.CM-3 Configuration Change Control

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Authorizes and documents changes to the Smart Grid information system;
2. Retains and reviews records of configuration-managed changes to the Smart Grid information system;
3. Audits activities associated with configuration-managed changes to the Smart Grid information system; and
4. Tests, validates, and documents configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system.

Supplemental Guidance

Configuration change control includes changes to the configuration settings for the Smart Grid information system and those IT products (e.g., operating systems, firewalls, routers) that are components of the Smart Grid information system. The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. Additionally, the organization develops procedures to preserve data during update actions to ensure continuity of operations and in case updates need to be “rolled back.”

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CM-3	High: SG.CM-3
-------------------	-------------------	---------------

SG.CM-4 Monitoring Configuration Changes

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization implements a process to monitor changes to the Smart Grid information system;
2. Prior to change implementation and as part of the change approval process, the organization analyzes changes to the Smart Grid information system for potential security impacts; and
3. After the Smart Grid information system is changed, the organization checks the security features to ensure that the features are still functioning properly.

Supplemental Guidance

Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional safeguards and countermeasures are required. The organization considers Smart Grid information system safety and security interdependencies.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-4	Moderate: SG.CM-4	High: SG.CM-4
--------------	-------------------	---------------

SG.CM-5 Access Restrictions for Configuration Change

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Defines, documents, and approves individual access privileges and enforces access restrictions associated with configuration changes to the Smart Grid information system;
2. Generates, retains, and reviews records reflecting all such changes;
3. Establishes terms and conditions for installing any hardware, firmware, or software on Smart Grid information system devices; and
4. Conducts audits of Smart Grid information system changes at an organization-defined frequency and if/when suspected unauthorized changes have occurred.

Supplemental Guidance

Planned or unplanned changes to the hardware, software, and/or firmware components of the Smart Grid information system may affect the overall security of the Smart Grid information system. Only authorized individuals should be allowed to obtain access to Smart Grid information system components for purposes of initiating changes, including upgrades, and modifications. Maintaining records is important for supporting after-the-fact actions should the organization become aware of an unauthorized change to the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CM-5	High: SG.CM-5
-------------------	-------------------	---------------

SG.CM-6 Configuration Settings

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Establishes configuration settings for components within the Smart Grid information system;
2. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures;
3. Documents changed configuration settings;
4. Identifies, documents, and approves exceptions from the configuration settings; and
5. Enforces the configuration settings in all components of the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings;
- A2. The organization employs automated mechanisms to respond to unauthorized changes to configuration settings; and
- A3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization’s incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

Impact Level Allocation

Low: SG.CM-6	Moderate: SG.CM-6	High: SG.CM-6
--------------	-------------------	---------------

SG.CM-7 Configuration for Least Functionality

Category: Common Technical Requirements, Integrity

Requirement

The organization -

1. Configures the Smart Grid information system to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally generated “prohibited and/or restricted” list; and
2. Reviews the Smart Grid information system on an organization-defined frequency or as deemed necessary to identify and restrict unnecessary functions, ports, protocols, and/or services.

Supplemental Guidance

Victoria Pillitteri 12/4/12 12:57 PM
Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 12:57 PM
Deleted: The organization c

Victoria Pillitteri 12/4/12 12:57 PM
Deleted: The organization r

The organization considers disabling unused or unnecessary physical and logical ports on Smart Grid information system components to prevent unauthorized connection of devices, and considers designing the overall system to enforce a policy of least functionality.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-7	Moderate: SG.CM-7	High: SG.CM-7
--------------	-------------------	---------------

SG.CM-8 Component Inventory

Category: Common Technical Requirements, Integrity

Requirement

The organization develops, documents, and maintains an inventory of the components of the Smart Grid information system that—

1. Accurately reflects the current Smart Grid information system configuration;
2. Provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability;
3. Identifies the roles responsible for component inventory;
4. Updates the inventory of system components as an integral part of component installations, system updates, and removals; and
5. Ensures that the location (logical and physical) of each component is included within the Smart Grid information system boundary.

Supplemental Guidance

The organization determines the appropriate level of granularity for any Smart Grid information system component included in the inventory that is subject to management control (e.g., tracking, reporting). The component inventory may also include a network diagram.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization updates the inventory of the information system components as an integral part of component installations and information system updates;
- A2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components; and
- A3. The organization employs automated mechanisms to detect the addition of unauthorized components or device into the environment and disables access by components or devices or notifies designated officials.

Impact Level Allocation

Low: SG.CM-8	Moderate: SG.CM-8	High: SG.CM-8
--------------	-------------------	---------------

SG.CM-9 Addition, Removal, and Disposal of Equipment

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization implements policy and procedures to address the addition, removal, and disposal of all Smart Grid information system equipment; and
2. All Smart Grid information system components and information are documented, identified, and tracked so that their location and function are known.

Supplemental Guidance

The policies and procedures should consider the sensitivity of critical security parameters such as passwords, cryptographic keys, and personally identifiable information such as name and social security numbers.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-9	Moderate: SG.CM-9	High: SG.CM-9
--------------	-------------------	---------------

SG.CM-10 Factory Default Settings Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization policy and procedures require the management of all factory default settings (e.g., authentication credentials, user names, configuration settings, and configuration parameters) on Smart Grid information system components and applications; and
2. The factory default settings should be changed upon installation and if used during maintenance.

Supplemental Guidance

Many Smart Grid information system devices and software are shipped with factory default settings to allow for initial installation and configuration.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization replaces default usernames whenever possible; and
- A2. Default passwords of applications, operating systems, database management systems, or other programs must be changed within an organizational-defined time period.

Impact Level Allocation

Low: SG.CM-10	Moderate: SG.CM-10	High: SG.CM-10
---------------	--------------------	----------------

SG.CM-11 Configuration Management Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops and implements a configuration management plan for the Smart Grid information system that—

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Defines the configuration items for the Smart Grid information system;
3. Defines when (in the system development life cycle) the configuration items are placed under configuration management;
4. Defines the means for uniquely identifying configuration items throughout the system development life cycle; and
5. Defines the process for managing the configuration of the controlled items.

Supplemental Guidance

The configuration management plan defines processes and procedures for how configuration management is used to support system development life cycle activities.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CM-11	Moderate: SG.CM-11	High: SG.CM-11
---------------	--------------------	----------------

3.12 CONTINUITY OF OPERATIONS (SG.CP)

Continuity of operations addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal system operation. The ability for the Smart Grid information system to function after an event is dependent on implementing continuity of operations policies, procedures, training, and resources. The security requirements recommended under the continuity of operations family provide policies and procedures for roles and responsibilities, training, testing, plan updates, alternate storage sites, alternate command and control methods, alternate control centers, recovery and reconstitution and fail-safe response.

SG.CP-1 Continuity of Operations Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented continuity of operations security policy that addresses—
 - i. The objectives, roles, and responsibilities for the continuity of operations security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the continuity of operations security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the continuity of operations security policy and associated continuity of operations protection requirements;
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
3. The organization ensures that the continuity of operations security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The continuity of operations policy can be included as part of the general information security policy for the organization. Continuity of operations procedures can be developed for the security program in general, and for a particular Smart Grid information system, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-1	Moderate: SG.CP-1	High: SG.CP-1
--------------	-------------------	---------------

SG.CP-2 Continuity of Operations Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system;
2. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring Smart Grid information system operations after a disruption or failure; and

- 3. A management authority reviews and approves the continuity of operations plan.

Supplemental Guidance

A continuity of operations plan addresses both business continuity planning and recovery of Smart Grid information system operations. Development of a continuity of operations plan is a process to identify procedures for safe Smart Grid information system operation while recovering from a Smart Grid information system disruption. The plan requires documentation of critical Smart Grid information system functions that need to be recovered.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization performs a root cause analysis for the event and submits any findings from the analysis to management.

Impact Level Allocation

Low: SG.CP-2	Moderate: SG.CP-2	High: SG.CP-2
--------------	-------------------	---------------

SG.CP-3 Continuity of Operations Roles and Responsibilities

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The continuity of operations plan—

- 1. Defines the roles and responsibilities of the various employees and contractors in the event of a significant incident; and
- 2. Identifies responsible personnel to lead the recovery and response effort if an incident occurs.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-3	Moderate: SG.CP-3	High: SG.CP-3
--------------	-------------------	---------------

SG.CP-4 Continuity of Operations Training

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

Victoria Pillitteri 12/4/12 12:59 PM
Comment [13]: Wrong font, table width/position on this impact level allocation.

The organization trains personnel in their continuity of operations roles and responsibilities with respect to the Smart Grid information system and provides refresher training on an organization-defined frequency.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-4	Moderate: SG.CP-4	High: SG.CP-4
--------------	-------------------	---------------

SG.CP-5 Continuity of Operations Plan Testing

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The continuity of operations plan is tested to determine its effectiveness and results are documented;
2. A management authority reviews the documented test results and initiates corrective actions, if necessary; and
3. The organization tests the continuity of operations plan for the Smart Grid information system on an organization-defined frequency, using defined tests.

Supplemental Guidance

None.

Requirement Enhancements

1. The organization coordinates continuity of operations plan testing and exercises with all affected organizational elements.

Additional Considerations

- A1. The organization employs automated mechanisms to test/exercise the continuity of operations plan; and
- A2. The organization tests/exercises the continuity of operations plan at the alternate processing site to familiarize Smart Grid information system operations personnel with the facility and available resources and to evaluate the site's capabilities to support continuity of operations.

Impact Level Allocation

Low: SG.CP-5	Moderate: SG. CP-5 (1)	High: SG. CP-5 (1)
--------------	------------------------	--------------------

SG.CP-6 Continuity of Operations Plan Update

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization reviews the continuity of operations plan for the Smart Grid information system and updates the plan to address Smart Grid information system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing on an organization-defined frequency.

Supplemental Guidance

Organizational changes include changes in mission, functions, or business processes supported by the Smart Grid information system. The organization communicates the changes to appropriate organizational elements.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-6	Moderate: SG.CP-6	High: SG.CP-6
--------------	-------------------	---------------

SG.CP-7 Alternate Storage Sites

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization determines the requirement for an alternate storage site and initiates any necessary agreements.

Supplemental Guidance

The Smart Grid information system backups and the transfer rate of backup information to the alternate storage site are performed on an organization-defined frequency.

Requirement Enhancements

1. The organization identifies potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions;
2. The organization identifies an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards; and
3. The organization configures the alternate storage site to facilitate timely and effective recovery operations.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CP-7 (1), (2)	High: SG.SG.CP-7 (1), (2), (3)
-------------------	----------------------------	--------------------------------

SG.CP-8 Alternate Telecommunication Services

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization identifies alternate telecommunication services for the Smart Grid information system and initiates necessary agreements to permit the resumption of operations for the safe operation of the Smart Grid information system within an organization-defined time period when the primary Smart Grid information system capabilities are unavailable.

Supplemental Guidance

Alternate telecommunication services required to resume operations within the organization-defined time period are either available at alternate organization sites or contracts with vendors need to be in place to support alternate telecommunication services for the Smart Grid information system.

Requirement Enhancements

1. Primary and alternate telecommunication service agreements contain priority-of-service provisions in accordance with the organization’s availability requirements;
2. Alternate telecommunication services do not share a single point of failure with primary telecommunication services;
3. Alternate telecommunication service providers need to be sufficiently separated from primary service providers so they are not susceptible to the same hazards; and
4. Primary and alternate telecommunication service providers need to have adequate contingency plans.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CP-8 (1), (4)	High: SG. CP-8 (1), (2), (3), (4)
-------------------	----------------------------	-----------------------------------

SG.CP-9 Alternate Control Center

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization identifies an alternate control center, necessary telecommunications, and initiates any necessary agreements to permit the resumption of Smart Grid information system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable.

Supplemental Guidance

Equipment, telecommunications, and supplies required to resume operations within the organization-prescribed time period need to be available at the alternative control center or by a contract in place to support delivery to the site.

Requirement Enhancements

1. The organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards;
2. The organization identifies potential accessibility problems to the alternate control center in the event of an area-wide disruption or disaster and outlines explicit mitigation actions; and
3. The organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization’s availability requirements.

Additional Considerations

- A1. The organization fully configures the alternate control center and telecommunications so that they are ready to be used as the operational site supporting a minimum required operational capability; and
- A2. The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

Impact Level Allocation

Low: Not Selected	Moderate: SG.CP-9 (1), (2), (3)	High: SG.CP-9 (1), (2), (3)
-------------------	---------------------------------	-----------------------------

SG.CP-10 Smart Grid Information System Recovery and Reconstitution

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides the capability to recover and reconstitute the Smart Grid information system to a known secure state after a disruption, compromise, or failure.

Supplemental Guidance

Smart Grid information system recovery and reconstitution to a known secure state means that—

1. All Smart Grid information system parameters (either default or organization-established) are set to secure values;
2. Security-critical patches are reinstalled;
3. Security-related configuration settings are reestablished;
4. Smart Grid information system documentation and operating procedures are available;
5. Application and Smart Grid information system software is reinstalled and configured with secure settings;
6. Information from the most recent, known secure backups is loaded; and
7. The Smart Grid information system is fully tested.

Requirement Enhancements

1. The organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state; and
2. The organization provides the capability to reimage Smart Grid information system components in accordance with organization-defined restoration time periods from configuration-controlled and integrity-protected media images representing a secure, operational state for the components.

Additional Considerations

None.

Impact Level Allocation

Low: SG.CP-10	Moderate: SG.CP-10 (1)	High: SG.CP-10 (1), (2)
---------------	------------------------	-------------------------

SG.CP-11 Fail-Safe Response

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other Smart Grid information systems or the loss of the Smart Grid information system itself.

Supplemental Guidance

In the event of a loss of communication between the Smart Grid information system and the operational facilities, the on-site instrumentation needs to be capable of executing a procedure that provides the maximum protection to the controlled infrastructure. For the electric sector, this may be to alert the operator of the failure and then do nothing (i.e., let the electric grid continue to operate). The organization defines what “loss of communications” means (e.g., 5 seconds or 5 minutes without communications). The organization then defines the appropriate fail-safe process for its industry.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system preserves the organization-defined state information in failure.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: SG.CP-11
-------------------	------------------------	----------------

3.13 IDENTIFICATION AND AUTHENTICATION (SG.IA)

Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a Smart Grid information system.

SG.IA-1 Identification and Authentication Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented identification and authentication security policy that addresses—
 - i. The objectives, roles, and responsibilities for the identification and authentication security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the identification and authentication security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements;
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
3. The organization ensures that the identification and authentication security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The identification and authentication policy can be included as part of the general security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IA-1	Moderate: SG.IA-1	High: SG.IA-1
--------------	-------------------	---------------

SG.IA-2 Identifier Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization receives authorization from a management authority to assign a user or device identifier.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization archives previous user or device identifiers; and
- A2. The organization selects an identifier that uniquely identifies an individual or device.

Impact Level Allocation

Low: SG.IA-2	Moderate: SG.IA-2	High: SG.IA-2
--------------	-------------------	---------------

SG.IA-3 Authenticator Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization manages Smart Grid information system authentication credentials for users and devices by—

1. Defining initial authentication credential content, such as defining password length and composition, tokens;
2. Establishing administrative procedures for initial authentication credential distribution; lost, compromised, or damaged authentication credentials; and revoking authentication credentials;
3. Changing/refreshing authentication credentials on an organization-defined frequency; and
4. Specifying measures to safeguard authentication credentials.

Supplemental Guidance

Measures to safeguard user authentication credentials include maintaining possession of individual authentication credentials, not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs automated tools to determine if authentication credentials are sufficiently strong to resist attacks intended to discover or otherwise compromise the authentication credentials; and
- A2. The organization requires unique authentication credentials be provided by vendors and manufacturers of Smart Grid information system components.

Impact Level Allocation

Low: SG.IA-3	Moderate: SG.IA-3	High: SG.IA-3
--------------	-------------------	---------------

SG.IA-4 User Identification and Authentication

Category: Unique Technical Requirements, [Integrity](#)

Requirement

The Smart Grid information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system uses multifactor authentication for—
- a. Remote access to non-privileged accounts;
 - b. Local access to privileged accounts; and
 - c. Remote access to privileged accounts.

Impact Level Allocation

Low: SG.IA-4	Moderate: SG.IA-4	High: SG.IA-4
--------------	-------------------	---------------

SG.IA-5 Device Identification and Authentication

Category: Unique Technical Requirements, [Integrity](#)

Requirement

The Smart Grid information system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection.

Supplemental Guidance

The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization.

Requirement Enhancements

1. The Smart Grid information system authenticates devices before establishing remote network connections using bidirectional authentication between devices that is cryptographically based; and
2. The Smart Grid information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.IA-5 (1), (2)	High: SG.IA-5 (1), (2)
-------------------	----------------------------	------------------------

SG.IA-6 Authenticator Feedback

Category: Unique Technical Requirements

Requirement

The authentication mechanisms in the Smart Grid information system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance

The Smart Grid information system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the Smart Grid information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IA-6	Moderate: SG.IA-6	High: SG.IA-6
--------------	-------------------	---------------

3.14 INFORMATION AND DOCUMENT MANAGEMENT (SG.ID)

Information and document management is generally a part of the organization records retention and document management system. Digital and hardcopy information associated with the development and execution of a Smart Grid information system is important and sensitive, and need to be managed. Smart Grid information system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive organization information and need to be protected. This information must be protected and verified that the appropriate versions are retained.

The following are the requirements for Information and Document Management that need to be supported and implemented by the organization to protect the Smart Grid information system.

SG.ID-1 Information and Document Management Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A Smart Grid information and document management policy that addresses—

- i. The objectives, roles and responsibilities for the information and document management security program as it relates to protecting the organization’s personnel and assets;
 - ii. The scope of the information and document management security program as it applies to all the organizational staff, contractors, and third parties;
 - iii. The retrieval of written and electronic records, equipment, and other media for the Smart Grid information system; and
 - iv. The destruction of written and electronic records, equipment, and other media for the Smart Grid information system; and
- b. Procedures to address the implementation of the information and document management security policy and associated Smart Grid information system information and document management protection requirements;
2. Management commitment ensures compliance of the organization’s security policy and other regulatory requirements; and
 3. The organization ensures that the Smart Grid information system information and document management policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The information and document management policy may be included as part of the general information security policy for the organization. The information and document management procedures can be developed for the security program in general and for a particular Smart Grid information system when required. The organization employs appropriate measures to ensure that long-term records and information can be retrieved (e.g., converting the data to a newer format, retaining older equipment that can read the data). Destruction includes the method of disposal such as shredding of paper records, erasing of disks or other electronic media, or physical destruction.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.ID-1	Moderate: SG.ID-1	High: SG.ID-1
--------------	-------------------	---------------

SG.ID-2 Information and Document Retention

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops policies and procedures detailing the retention of organization information;

2. The organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations;
3. The organization manages Smart Grid information system-related data including establishing retention policies and procedures for both electronic and paper data; and
4. The organization manages access to Smart Grid information system-related data based on assigned roles and responsibilities.

Supplemental Guidance

The retention procedures address retention/destruction issues for all applicable information media.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.ID-2	Moderate: SG.ID-2	High: SG.ID-2
--------------	-------------------	---------------

SG.ID-3 Information Handling

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops and reviews the policies and procedures detailing the handling of information on an organization-defined frequency.

Supplemental Guidance

Written policies and procedures detail access, sharing, copying, transmittal, distribution, and disposal or destruction of Smart Grid information system information. These policies or procedures include the periodic review of all information to ensure that it is properly handled.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.ID-3	Moderate: SG.ID-3	High: SG.ID-3
--------------	-------------------	---------------

SG.ID-4 Information Exchange

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

Victoria Pillitteri 12/4/12 1:00 PM
Comment [14]: Rephrased into active voice, no content change.

Victoria Pillitteri 12/4/12 1:00 PM
Deleted: Organization-implemented policies and procedures detailing the handling of information are developed and reviewed on an

Agreements are established for the exchange of information, firmware, and software between the organization and external parties such as third parties, vendors and contractors.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. If a specific device needs to communicate with another device outside the Smart Grid information system, communications need to be limited to only the devices that need to communicate.

Impact Level Allocation

Low: SG.ID-4	Moderate: SG.ID-4	High: SG.ID-4
--------------	-------------------	---------------

SG.ID-5 Automated Labeling

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The Smart Grid information system automatically labels information in storage, in process, and in transmission in accordance with—

1. Access control requirements;
2. Special dissemination, handling, or distribution instructions; and
3. Otherwise as required by the Smart Grid information system security policy.

Supplemental Guidance

Automated labeling refers to labels employed on internal data structures (e.g., records, buffers, files) within the Smart Grid information system. Such labels are often used to implement access control and flow control policies.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system maintains the binding of the label to the information.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

3.15 INCIDENT RESPONSE (SG.IR)

Incident response addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal Smart Grid information system operation. Incident response entails the preparation, testing, and maintenance of specific policies

and procedures to enable the organization to recover the Smart Grid information system's operational status after the occurrence of a disruption. Disruptions can come from natural disasters, such as earthquakes, tornados, floods, or from manmade events like riots, terrorism, or vandalism. The ability for the Smart Grid information system to function after such an event is directly dependent on implementing policies, procedures, training, and resources in place ahead of time using the organization's planning process. The security requirements recommended under the incident response family provide policies and procedures for incident response monitoring, handling, reporting, testing, training, recovery, and reconstitution of the Smart Grid information systems for an organization.

SG.IR-1 Incident Response Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

- 1.** The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented incident response security policy that addresses—
 - i. The objectives, roles, and responsibilities for the incident response security program as it relates to protecting the organization's personnel and assets; and
 - ii. The scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the incident response security policy and associated incident response protection requirements;
- 2.** Management commitment ensures compliance with the organization's security policy and other regulatory requirements;
- 3.** The organization ensures that the incident response security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations; and
- 4.** The organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood."

Supplemental Guidance

The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular Smart Grid information system, when required. The various types of incidents that may result from system intrusion need to be identified and classified as to their effects and likelihood so that a proper response can be formulated for each potential incident. The organization determines the impact to each Smart Grid system and the consequences associated with loss of one or more of the Smart Grid information systems.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-1	Moderate: SG.IR-1	High: SG.IR-1
--------------	-------------------	---------------

SG.IR-2 Incident Response Roles and Responsibilities

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization’s Smart Grid information system security plan defines the specific roles and responsibilities in relation to various types of incidents; and
2. The plan identifies responsible personnel to lead the response effort if an incident occurs. Response teams need to be formed, including Smart Grid information system and other process owners, to reestablish operations.

Supplemental Guidance

The organization’s Smart Grid information system security plan defines the roles and responsibilities of the various employees, contractors, and third parties in the event of an incident. The response teams have a major role in the interruption identification and planning process.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-2	Moderate: SG.IR-2	High: SG.IR-2
--------------	-------------------	---------------

SG.IR-3 Incident Response Training

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

Personnel are trained in their incident response roles and responsibilities with respect to the Smart Grid information system and receive refresher training on an organization-defined frequency.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization incorporates Smart Grid information system simulated events into continuity of operations training to facilitate effective response by personnel in crisis situations; and
- A2. The organization employs automated mechanisms to provide a realistic Smart Grid information system training environment.

Impact Level Allocation

Low: SG.IR-3	Moderate: SG.IR-3	High: SG.IR-3
--------------	-------------------	---------------

SG.IR-4 Incident Response Testing and Exercises

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization tests and/or exercises the incident response capability for the information system at an organization-defined frequency using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability

Victoria Pillitteri 12/4/12 1:02 PM
Comment [15]: This number was missing

Impact Level Allocation

Low: SG.IR-4	Moderate: SG.IR-4	High: SG.IR-4
--------------	-------------------	---------------

SG.IR-5 Incident Handling

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, mitigation, and recovery;
2. Integrates incident handling procedures with continuity of operations procedures; and
3. Incorporates lessons learned from incident handling activities into incident response procedures.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs automated mechanisms to administer and support the incident handling process.

Impact Level Allocation

Low: SG.IR-5	Moderate: SG.IR-5	High: SG.IR-5
--------------	-------------------	---------------

SG.IR-6 Incident Monitoring

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization tracks and documents Smart Grid information system and network security incidents.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Impact Level Allocation

Low: SG.IR-6	Moderate: SG.IR-6	High: SG.IR-6
--------------	-------------------	---------------

SG.IR-7 Incident Reporting

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization incident reporting procedure includes:
 - a. What is a reportable incident;
 - b. The granularity of the information reported;
 - c. Who receives the report; and
 - d. The process for transmitting the incident information.
2. Detailed incident data is reported in a manner that complies with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to assist in the reporting of security incidents.

Impact Level Allocation

Low: SG.IR-7	Moderate: SG.IR-7	High: SG.IR-7
--------------	-------------------	---------------

SG.IR-8 Incident Response Investigation and Analysis

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization -

1. Develops and implements policies and procedures include an incident response investigation and analysis program;
2. Includes investigation and analysis of Smart Grid information system incidents in the planning process; and
3. Develops, tests, deploys, and documents an incident investigation and analysis process.

Supplemental Guidance

The organization documents its policies and procedures to show that investigation and analysis of incidents are included in the planning process. The procedures ensure that the Smart Grid information system is capable of providing event data to the proper personnel for analysis and for developing mitigation steps.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-8	Moderate: SG.IR-8	High: SG.IR-8
--------------	-------------------	---------------

SG.IR-9 Corrective Action

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization -

1. Reviews investigation results and determines corrective actions needed; and
2. Includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of cyber security and Smart Grid information system incidents are fully implemented.

Victoria Pillitteri 12/4/12 1:02 PM
Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 1:02 PM
Deleted: The organization p

Victoria Pillitteri 12/4/12 1:03 PM
Deleted: The organization i

Victoria Pillitteri 12/4/12 1:03 PM
Deleted: The organization d

Victoria Pillitteri 12/4/12 1:04 PM
Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 1:04 PM
Deleted: The organization r

Victoria Pillitteri 12/4/12 1:04 PM
Deleted: The organization i

Supplemental Guidance

The organization encourages and promotes cross-industry incident information exchange and cooperation to learn from the experiences of others.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-9	Moderate: SG.IR-9	High: SG.IR-9
--------------	-------------------	---------------

SG.IR-10 Smart Grid Information System Backup

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Conducts backups of user-level information contained in the Smart Grid information system on an organization-defined frequency;
2. Conducts backups of Smart Grid information system-level information (including Smart Grid information system state information) contained in the Smart Grid information system on an organization-defined frequency;
3. Conducts backups of information system documentation including security-related documentation on an organization-defined frequency consistent with recovery time; and
4. Protects the confidentiality and integrity of backup information at the storage location.

Supplemental Guidance

The protection of Smart Grid information system backup information while in transit is beyond the scope of this requirement.

Requirement Enhancements

1. The organization tests backup information at an organization-defined frequency to verify media reliability and information integrity;
2. The organization selectively uses backup information in the restoration of Smart Grid information system functions as part of continuity of operations testing; and
3. The organization stores backup copies of the operating system and other critical Smart Grid information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-10	Moderate: SG.IR-10 (1)	High: SG.IR-10 (1), (2), (3)
---------------	------------------------	------------------------------

SG.IR-11 Coordination of Emergency Response

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization’s security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.

Supplemental Guidance

The organization expands relationships with local emergency response personnel to include information sharing and coordinated response to cyber security incidents.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.IR-11	Moderate: SG.IR-11	High: SG.IR-11
---------------	--------------------	----------------

3.16 SMART GRID INFORMATION SYSTEM DEVELOPMENT AND MAINTENANCE (SG.MA)

Security is most effective when it is designed into the Smart Grid information system and sustained, through effective maintenance, throughout the life cycle of the Smart Grid information system. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a Smart Grid information system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.

SG.MA-1 Smart Grid Information System Maintenance Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented Smart Grid information system maintenance security policy that addresses—
 - i. The objectives, roles, and responsibilities for the Smart Grid information system maintenance security program as it relates to protecting the organization’s personnel and assets; and

- ii. The scope of the Smart Grid information system maintenance security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the Smart Grid information system maintenance security policy and associated Smart Grid information system maintenance protection requirements;
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
 3. The organization ensures that the Smart Grid information system maintenance security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The Smart Grid information system maintenance policy can be included as part of the general information security policy for the organization. Smart Grid information system maintenance procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MA-1	Moderate: SG.MA-1	High: SG.MA-1
--------------	-------------------	---------------

SG.MA-2 Legacy Smart Grid Information System Upgrades

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops policies and procedures to upgrade existing legacy Smart Grid information systems to include security mitigating measures commensurate with the organization’s risk tolerance and the risk to the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MA-2	Moderate: SG.MA-2	High: SG.MA-2
--------------	-------------------	---------------

SG.MA-3 Smart Grid Information System Maintenance

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

- 1.** Schedules, performs, documents, and reviews records of maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- 2.** Explicitly approves the removal of the Smart Grid information system or Smart Grid information system components from organizational facilities for off-site maintenance or repairs;
- 3.** Sanitizes the equipment to remove all critical/sensitive information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
- 4.** Checks all potentially impacted security requirements to verify that the requirements are still functioning properly following maintenance or repair actions; and
- 5.** Makes and secures backups of critical Smart Grid information system software, applications, and data for use if the operating system becomes corrupted or destroyed.

Supplemental Guidance

All maintenance activities to include routine, scheduled maintenance and repairs, and unplanned maintenance are controlled, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Maintenance procedures that require the physical removal of any Smart Grid information system component needs to be documented, listing the date, time, reason for removal, estimated date of reinstallation, and name personnel removing components.

Requirement Enhancements

- 1.** The organization maintains maintenance records for the Smart Grid information system that include:
 - a. The date and time of maintenance;
 - b. Name of the individual performing the maintenance;
 - c. Name of escort, if necessary;
 - d. A description of the maintenance performed; and
 - e. A list of equipment removed or replaced (including identification numbers, if applicable).

Additional Considerations

- A1. The organization employs automated mechanisms to schedule and document maintenance and repairs as required, producing up-to-date, accurate, complete, and available records of all maintenance and repair actions needed, in process, and completed.

Impact Level Allocation

Low: SG.MA-3	Moderate: SG.MA-3	High: SG.MA-3 (1)
--------------	-------------------	-------------------

SG.MA-4 Maintenance Tools

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization approves and monitors the use of Smart Grid information system maintenance tools.

Supplemental Guidance

The requirement addresses security-related issues when the hardware, firmware, and software are brought into the Smart Grid information system for diagnostic and repair actions.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization requires approval from a management authority explicitly authorizing removal of equipment from the facility;
- A2. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications;
- A3. The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the Smart Grid information system; and
- A4. The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

Impact Level Allocation

Low: SG.MA-4	Moderate: SG.MA-4	High: SG.MA-4
--------------	-------------------	---------------

SG.MA-5 Maintenance Personnel

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

- 1. The organization documents authorization and approval policies and procedures for maintaining a list of personnel authorized to perform maintenance on the Smart Grid information system; and
- 2. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the Smart Grid information system.

Supplemental Guidance

Maintenance personnel need to have appropriate access authorization to the Smart Grid information system when maintenance activities allow access to organizational information that could result in a future compromise of availability, integrity, or confidentiality.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MA-5	Moderate: SG.MA-5	High: SG.MA-5
--------------	-------------------	---------------

SG.MA-6 Remote Maintenance

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization policy and procedures for remote maintenance include:

1. Authorization and monitoring the use of remote maintenance and diagnostic activities;
2. Use of remote maintenance and diagnostic tools;
3. Maintenance records for remote maintenance and diagnostic activities;
4. Termination of all remote maintenance sessions; and
5. Management of authorization credentials used during remote maintenance.

Supplemental Guidance

None.

Requirement Enhancements

1. The organization requires that remote maintenance or diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the Smart Grid information system being serviced; or
2. The organization removes the component to be serviced from the Smart Grid information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities and after the service is performed, sanitizes the component (with regard to potentially malicious software) before returning the component to the Smart Grid information system.

Additional Considerations

- A1. The organization requires that remote maintenance sessions are protected through the use of a strong authentication credential; and
- A2. The organization requires that (a) maintenance personnel notify the Smart Grid information system administrator when remote maintenance is planned (e.g., date/time), and (b) a management authority approves the remote maintenance.

Impact Level Allocation

Low: SG.MA-6	Moderate: SG.MA-6	High: SG.MA-6 (1)
--------------	-------------------	-------------------

Victoria Pillitteri 12/4/12 1:07 PM
Deleted: [1]

Victoria Pillitteri 12/4/12 1:06 PM
Deleted: R

Victoria Pillitteri 12/4/12 1:10 PM
Deleted: R

Victoria Pillitteri 12/4/12 1:07 PM
Formatted: Numbered + Level: 1 +
Numbering Style: 1, 2, 3, ... + Start at: 1 +
Alignment: Left + Aligned at: 0.25" + Tab
after: 0.5" + Indent at: 0.5"

SG.MA-7 Timely Maintenance

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization obtains maintenance support and spare parts for an organization-defined list of security-critical Smart Grid information system components.

Supplemental Guidance

The organization specifies those Smart Grid information system components that, when not operational, result in increased risk to organizations or individuals because the security functionality intended by that component is not being provided.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MA-7	Moderate: SG.MA-7	High: SG.MA-7
--------------	-------------------	---------------

3.17 MEDIA PROTECTION (SG.MP)

The security requirements under the media protection family provide policy and procedures for limiting access to media to authorized users. Security measures also exist for distribution and handling requirements as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media. Media assets include compact discs; digital video discs; erasable, programmable read-only memory; tapes; printed reports; and documents.

SG.MP-1 Media Protection Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented media protection security policy that addresses—
 - i. The objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the media protection security policy and associated media protection requirements;
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and

- 3. The organization ensures that the media protection security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The media protection policy can be included as part of the general security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MP-1	Moderate: SG.MP-1	High: SG.MP-1
--------------	-------------------	---------------

SG.MP-2 Media Sensitivity Level

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The sensitivity level of media indicates the protection required commensurate with the impact of compromise.

Supplemental Guidance

These media sensitivity levels provide guidance for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MP-2	Moderate: SG.MP-2	High: SG.MP-2
--------------	-------------------	---------------

SG.MP-3 Media Marking

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization marks removable Smart Grid information system media and Smart Grid information system output in accordance with organization-defined policy and procedures.

Supplemental Guidance

Smart Grid information system markings refer to the markings employed on external media (e.g., video displays, hardcopy documents output from the Smart Grid information system).

External markings are distinguished from internal markings (i.e., the labels used on internal data structures within the Smart Grid information system).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.MP-3	High: SG.MP-3
-------------------	-------------------	---------------

SG.MP-4 Media Storage

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization physically manages and stores Smart Grid information system media within protected areas. The sensitivity of the material determines how the media are stored.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MP-4	Moderate: SG.MP-4	High: SG.MP-4
--------------	-------------------	---------------

SG.MP-5 Media Transport

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Protects organization-defined types of media during transport outside controlled areas using organization-defined security measures;
2. Maintains accountability for Smart Grid information system media during transport outside controlled areas; and
3. Restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance

A controlled area is any space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs an identified custodian throughout the transport of Smart Grid information system media; and
- A2. The organization documents activities associated with the transport of Smart Grid information system media using an organization-defined Smart Grid information system of records.

Impact Level Allocation

Low: SG.MP-5	Moderate: SG.MP-5	High: SG.MP-5
--------------	-------------------	---------------

SG.MP-6 Media Sanitization and Disposal

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization sanitizes Smart Grid information system media before disposal or release for reuse. The organization tests sanitization equipment and procedures to verify correct performance on an organization-defined frequency.

Supplemental Guidance

Sanitization is the process of removing information from media such that data recovery is not possible.

Requirement Enhancements

1. The organization tracks, documents, and verifies media sanitization and disposal actions.

Additional Considerations

None.

Impact Level Allocation

Low: SG.MP-6	Moderate: SG.MP-6 (1)	High: SG.MP-6 (1)
--------------	-----------------------	-------------------

Victoria Pillitteri 12/4/12 1:14 PM

Comment [16]: This was missing the number.

Victoria Pillitteri 12/4/12 1:13 PM

Formatted: NumList, Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Victoria Pillitteri 12/4/12 1:14 PM

Deleted: Environmental security addresses the safety of assets from damage from environmental concerns.

3.18 PHYSICAL AND ENVIRONMENTAL SECURITY (SG.PE)

Physical and environmental security encompasses protection of physical assets from damage, misuse, or theft. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access Smart Grid information systems and components. Physical and environmental security addresses protection from environmental threats.

SG.PE-1 Physical and Environmental Security Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented physical and environmental security policy that addresses—
 - i. The objectives, roles, and responsibilities for the physical and environmental security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the physical and environmental security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the physical and environmental security policy and associated physical and environmental protection requirements;
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
3. The organization ensures that the physical and environmental security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The organization may include the physical and environmental security policy as part of the general security policy for the organization.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-1	Moderate: SG.PE-1	High: SG.PE-1
--------------	-------------------	---------------

SG.PE-2 Physical Access Authorizations

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops and maintains lists of personnel with authorized access to facilities containing Smart Grid information systems and issues appropriate authorization credentials (e.g., badges, identification cards); and
2. Designated officials within the organization review and approve access lists on an organization-defined frequency, removing from the access lists personnel no longer requiring access.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization authorizes physical access to the facility where the Smart Grid information system resides based on position or role;
- A2. The organization requires multiple forms of identification to gain access to the facility where the Smart Grid information system resides; and
- A3. The organization requires multifactor authentication to gain access to the facility where the Smart Grid information system resides.

Impact Level Allocation

Low: SG.PE-2	Moderate: SG.PE-2	High: SG.PE-2
--------------	-------------------	---------------

SG.PE-3 Physical Access

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Enforces physical access authorizations for all physical access points to the facility where the Smart Grid information system resides;
2. Verifies individual access authorizations before granting access to the facility;
3. Controls entry to facilities containing Smart Grid information systems;
4. Secures keys, combinations, and other physical access devices;
5. Inventories physical access devices on a periodic basis; and
6. Changes combinations, keys, and authorization credentials on an organization-defined frequency and when keys are lost, combinations are compromised, individual credentials are lost, or individuals are transferred or terminated.

Supplemental Guidance

Physical access devices include keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational Smart Grid information system may be located in areas designated as publicly accessible with access to such devices being safeguarded.

Requirement Enhancements

1. The organization requires physical access mechanisms to Smart Grid information system assets in addition to physical access mechanisms to the facility; and
2. The organization employs hardware to deter unauthorized physical access to Smart Grid information system devices.

Additional Considerations

- A1. The organization ensures that every physical access point to the facility where the Smart Grid information system resides is guarded or alarmed and monitored on an organization-defined frequency.

Impact Level Allocation

Low: SG.PE-3	Moderate: SG.PE-3 (2)	High: SG.PE-3 (1), (2)
--------------	-----------------------	------------------------

SG.PE-4 Monitoring Physical Access

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Monitors physical access to the Smart Grid information system to detect and respond to physical security incidents;
2. Reviews physical access logs on an organization-defined frequency;
3. Coordinates results of reviews and investigations with the organization’s incident response capability; and
4. Ensures that investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization’s incident response capability.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization installs and monitors real-time physical intrusion alarms and surveillance equipment; and
- A2. The organization implements automated mechanisms to recognize potential intrusions and initiates designated response actions.

Impact Level Allocation

Low: SG.PE-4	Moderate: SG.PE-4	High: SG.PE-4
--------------	-------------------	---------------

SG.PE-5 Visitor Control

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization controls physical access to the Smart Grid information system by authenticating visitors before authorizing access to the facility.

Supplemental Guidance

Contractors and others with permanent authorization credentials are not considered visitors.

Requirement Enhancements

- 1. The organization escorts visitors and monitors visitor activity as required according to security policies and procedures.

Additional Considerations

A1. The organization requires multiple forms of identification for access to the facility.

Impact Level Allocation

Low: SG.PE-5	Moderate: SG.PE-5 (1)	High: SG.PE-5 (1)
--------------	-----------------------	-------------------

SG.PE-6 Visitor Records

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization maintains visitor access records to the facility that include:

- 1. Name and organization of the person visiting;
- 2. Signature of the visitor;
- 3. Form of identification;
- 4. Date of access;
- 5. Time of entry and departure;
- 6. Purpose of visit; and
- 7. Name and organization of person visited.

Designated officials within the organization review the access logs after closeout and periodically review access logs based on an organization-defined frequency.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization employs automated mechanisms to facilitate the maintenance and review of access records.

Impact Level Allocation

Low: SG.PE-6	Moderate: SG.PE-6	High: SG.PE-6
--------------	-------------------	---------------

SG.PE-7 Physical Access Log Retention

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

Victoria Pillitteri 12/4/12 1:14 PM
Comment [17]: Was missing the number.
Victoria Pillitteri 12/4/12 1:14 PM
Formatted: NumList, Numbered + Level:
1 + Numbering Style: 1, 2, 3, ... + Start at:
1 + Alignment: Left + Aligned at: 0.25" +
Tab after: 0.5" + Indent at: 0.5"

The organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-7	Moderate: SG.PE-7	High: SG.PE-7
--------------	-------------------	---------------

SG.PE-8 Emergency Shutoff Protection

Category: Common Technical Requirements, Availability

Requirement

The organization protects the emergency power-off capability from accidental and intentional/unauthorized activation.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-8	Moderate: SG.PE-8	High: SG.PE-8
--------------	-------------------	---------------

SG.PE-9 Emergency Power

Category: Common Technical Requirements, Availability

Requirement

The organization provides an alternate power supply to facilitate an orderly shutdown of noncritical Smart Grid information system components in the event of a primary power source loss.

Supplemental Guidance

None.

Victoria Pillitteri 12/4/12 1:15 PM
Deleted: Governance, Risk, and Compliance (GRC)

Victoria Pillitteri 12/4/12 1:16 PM
Deleted: Governance, Risk, and Compliance (GRC)

Requirement Enhancements

1. The organization provides a long-term alternate power supply for the Smart Grid information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Additional Considerations

- A1. The organization provides a long-term alternate power supply for the Smart Grid information system that is self-contained and not reliant on external power generation.

Impact Level Allocation

Low: SG.PE-9	Moderate: SG.PE-9 (1)	High: SG.PE-9 (1)
--------------	-----------------------	-------------------

SG.PE-10 Delivery and Removal

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization authorizes, monitors, and controls organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items.

Supplemental Guidance

The organization secures delivery areas and, if possible, isolates delivery areas from the Smart Grid information system to avoid unauthorized physical access.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-10	Moderate: SG.PE-10	High: SG.PE-10
---------------	--------------------	----------------

SG.PE-11 Alternate Work Site

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization -

1. Establishes an alternate work site (for example, private residences) with proper equipment and communication infrastructure to compensate for the loss of the primary work site; and
2. Implements appropriate management, operational, and technical security measures at alternate control centers.

Victoria Pillitteri 12/4/12 1:16 PM
Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 1:16 PM
Deleted: The organization e

Victoria Pillitteri 12/4/12 1:16 PM
Deleted: The organization i

Supplemental Guidance

The organization may define different sets of security requirements for specific alternate work sites or types of sites.

Requirement Enhancements

None.

Additional Considerations

A1. The organization provides methods for employees to communicate with Smart Grid information system security staff in case of security problems.

Impact Level Allocation

Low: SG.PE-11	Moderate: SG.PE-11	High: SG.PE-11
---------------	--------------------	----------------

SG.PE-12 Location of Smart Grid Information System Assets

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization locates Smart Grid information system assets to minimize potential damage from physical and environmental hazards.

Supplemental Guidance

Physical and environmental hazards include flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation.

Requirement Enhancements

1. The organization considers the risk associated with physical and environmental hazards when planning new Smart Grid information system facilities or reviewing existing facilities.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PE-12	Moderate: SG.PE-12	High: SG.PE-12 (1)
---------------	--------------------	--------------------

3.19 PLANNING (SG.PL)

The purpose of strategic planning is to maintain optimal operations and to prevent or recover from undesirable interruptions to Smart Grid information system operation. Interruptions may take the form of a natural disaster (hurricane, tornado, earthquake, flood, etc.), an unintentional manmade event (accidental equipment damage, fire or explosion, operator error, etc.), an intentional manmade event (attack by bomb, firearm or vandalism, hacker or malware, etc.), or an equipment failure. The types of planning considered are security planning to prevent undesirable interruptions, continuity of operations planning to maintain Smart Grid information system operation during and after an interruption, and planning to identify mitigation strategies.

SG.PL-1 Strategic Planning Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented planning policy that addresses—
 - i. The objectives, roles, and responsibilities for the planning program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the planning program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the planning policy and associated strategic planning requirements;
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
3. The organization ensures that the planning policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The strategic planning policy may be included as part of the general information security policy for the organization. Strategic planning procedures may be developed for the security program in general and a Smart Grid information system in particular, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PL-1	Moderate: SG.PL-1	High: SG.PL-1
--------------	-------------------	---------------

SG.PL-2 Smart Grid Information System Security Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Develops a security plan for each Smart Grid information system that—
 - a. Aligns with the organization’s enterprise architecture;
 - b. Explicitly defines the components of the Smart Grid information system;
 - c. Describes relationships with and interconnections to other Smart Grid information systems;

- d. Provides an overview of the security objectives for the Smart Grid information system;
 - e. Describes the security requirements in place or planned for meeting those requirements; and
 - f. Is reviewed and approved by the management authority prior to plan implementation;
2. Reviews the security plan for the Smart Grid information system on an organization-defined frequency; and
 3. Revises the plan to address changes to the Smart Grid information system/environment of operation or problems identified during plan implementation or security requirement assessments.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PL-2	Moderate: SG.PL-2	High: SG.PL-2
--------------	-------------------	---------------

SG.PL-3 Rules of Behavior

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes and makes readily available to all Smart Grid information system users, a set of rules that describes their responsibilities and expected behavior with regard to Smart Grid information system usage.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial Web sites, and sharing Smart Grid information system account information; and
- A2. The organization obtains signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the Smart Grid information system.

Impact Level Allocation

Low: SG.PL-3	Moderate: SG.PL-3	High: SG.PL-3
--------------	-------------------	---------------

SG.PL-4 Privacy Impact Assessment

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization conducts a privacy impact assessment on the Smart Grid information system; and
2. The privacy impact assessment is reviewed and approved by a management authority.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PL-4	Moderate: SG.PL-4	High: SG.PL-4
--------------	-------------------	---------------

SG.PL-5 Security-Related Activity Planning

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization plans and coordinates security-related activities affecting the Smart Grid information system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals; and
2. Organizational planning and coordination includes both emergency and nonemergency (e.g., routine) situations.

Supplemental Guidance

Routine security-related activities include, but are not limited to, security assessments, audits, Smart Grid information system hardware, firmware, and software maintenance, and testing/exercises.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.PL-5	High: SG.PL-5
-------------------	-------------------	---------------

3.20 SECURITY PROGRAM MANAGEMENT (SG.PM)

The security program lays the groundwork for securing the organization’s enterprise and Smart Grid information system assets. Security procedures define how an organization implements the security program.

SG.PM-1 Security Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented security program security policy that addresses—
 - i. The objectives, roles, and responsibilities for the security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the security program security policy and associated security program protection requirements;
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
3. The organization ensures that the security program security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The information system security policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for the information system in particular, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-1	Moderate: SG.PM-1	High: SG.PM-1
--------------	-------------------	---------------

SG.PM-2 Security Program Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops and disseminates an organization-wide security program plan that—
 - a. Provides an overview of the requirements for the security program and a description of the security program management requirements in place or planned for meeting those program requirements;
 - b. Provides sufficient information about the program management requirements to enable an implementation that is compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
 - c. Includes roles, responsibilities, management accountability, coordination among organizational entities, and compliance; and
 - d. Is approved by a management authority with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, and individuals;
2. Reviews the organization-wide security program plan on an organization-defined frequency; and
3. Revises the plan to address organizational changes and problems identified during plan implementation or security requirement assessments.

Supplemental Guidance

The security program plan documents the organization-wide program management requirements. The security plans for individual information systems and the organization-wide security program plan together, provide complete coverage for all security requirements employed within the organization.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-2	Moderate: SG.PM-2	High: SG.PM-2
--------------	-------------------	---------------

SG.PM-3 Senior Management Authority

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization appoints a senior management authority with the responsibility for the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-3	Moderate: SG.PM-3	High: SG.PM-3
--------------	-------------------	---------------

SG.PM-4 Security Architecture

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops a security architecture with consideration for the resulting risk to organizational operations, organizational assets, individuals, and other organizations.

Supplemental Guidance

The integration of security requirements into the organization’s enterprise architecture helps to ensure that security considerations are addressed by organizations early in the information system development life cycle.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-4	Moderate: SG.PM-4	High: SG.PM-4
--------------	-------------------	---------------

SG.PM-5 Risk Management Strategy

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems; and
2. Implements that strategy consistently across the organization.

Supplemental Guidance

An organization-wide risk management strategy should include a specification of the risk tolerance of the organization, guidance on acceptable risk assessment methodologies, and a process for consistently evaluating risk across the organization.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-5	Moderate: SG.PM-5	High: SG.PM-5
--------------	-------------------	---------------

SG.PM-6 Security Authorization to Operate Process

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Manages (e.g., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; and
2. Fully integrates the security authorization to operate processes into an organization-wide risk management strategy.

Supplemental Guidance

None.

Requirement Enhancements

None.

Impact Level Allocation

Low: SG.PM-6	Moderate: SG.PM-6	High: SG.PM-6
--------------	-------------------	---------------

SG.PM-7 Mission/Business Process Definition

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization defines mission/business processes that include consideration for security and the resulting risk to organizational operations, organizational assets, and individuals.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-7	Moderate: SG.PM-7	High: SG.PM-7
--------------	-------------------	---------------

SG.PM-8 Management Accountability

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization defines a framework of management accountability that establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PM-8	Moderate: SG.PM-8	High: SG.PM-8
--------------	-------------------	---------------

3.21 PERSONNEL SECURITY (SG.PS)

Personnel security addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination. The organization screens applicants for critical positions in the operation and maintenance of the Smart Grid information system. The organization may consider implementing a confidentiality or nondisclosure agreement that employees and third-party users of facilities must sign before being granted access to the Smart Grid information system. The organization also documents and implements a process to secure resources and revoke access privileges when personnel terminate.

SG.PS-1 Personnel Security Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented personnel security policy that addresses—
 - i. The objectives, roles, and responsibilities for the personnel security program as it relates to protecting the organization's personnel and assets; and
 - ii. The scope of the personnel security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the personnel security policy and associated personnel protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and

- 3. The organization ensures that the personnel security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The personnel security policy may be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular Smart Grid information system, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-1	Moderate: SG.PS-1	High: SG.PS-1
--------------	-------------------	---------------

SG.PS-2 Position Categorization

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization =

1. Assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions;
2. Reviews and revises position risk designations; and
3. Determines the frequency of the review based on the internal requirements or regulatory commitments.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-2	Moderate: SG.PS-2	High: SG.PS-2
--------------	-------------------	---------------

SG.PS-3 Personnel Screening

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization =

Victoria Pillitteri 12/4/12 2:40 PM
Deleted:

Victoria Pillitteri 12/4/12 2:43 PM
Formatted: NumList, Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Victoria Pillitteri 12/4/12 2:40 PM
Deleted: a

Victoria Pillitteri 12/4/12 2:40 PM
Deleted: . The organization r

Victoria Pillitteri 12/4/12 2:40 PM
Formatted: NumList

Victoria Pillitteri 12/4/12 2:40 PM
Deleted: . The organization d

Victoria Pillitteri 12/4/12 2:40 PM
Deleted: organization's

1. Screens individuals requiring access to the Smart Grid information system before access is authorized; and

1. Maintains consistency between the screening process and organization-defined policy, regulations, guidance, and the criteria established for the risk designation of the assigned position.

Supplemental Guidance

Basic screening requirements should include:

1. Employment history;
2. Verification of the highest education degree received;
3. Residency;
4. References; and
5. Law enforcement records.

Requirement Enhancements

None.

Additional Considerations

A1. The organization rescreens individuals with access to Smart Grid information systems based on a defined list of conditions requiring rescreening and the frequency of such rescreening.

Impact Level Allocation

Low: SG.PS-3	Moderate: SG.PS-3	High: SG.PS-3
--------------	-------------------	---------------

SG.PS-4 Personnel Termination

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization -

1. Revokes logical and physical access to facilities and systems, and ensures that all organization-owned property is returned when an employee is terminated. Organization-owned documents relating to the Smart Grid information system that are in the employee's possession are transferred to the new authorized owner;
2. Terminates all logical and physical on an organization-defined time frame for personnel terminated for cause; and
3. Conducts exit interviews to ensure that individuals understand any security constraints imposed by being a former employee and that proper accountability is achieved for all Smart Grid information system-related property.

Supplemental Guidance

Organization-owned property includes Smart Grid information system administration manuals, keys, identification cards, building passes, computers, cell phones, and personal data assistants.

Victoria Pillitteri 12/4/12 2:42 PM

Deleted:

Victoria Pillitteri 12/4/12 2:42 PM

Deleted: s

Victoria Pillitteri 12/4/12 2:42 PM

Formatted: NumList, Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Victoria Pillitteri 12/4/12 2:42 PM

Deleted: . The organization m

Victoria Pillitteri 12/4/12 2:43 PM

Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 2:43 PM

Deleted: When an employee is terminated, the organization r

Victoria Pillitteri 12/4/12 2:44 PM

Deleted: A

Victoria Pillitteri 12/4/12 2:44 PM

Deleted: access must be terminated at

Victoria Pillitteri 12/4/12 2:44 PM

Deleted: E

Organization-owned documents include field device configuration and operational information and Smart Grid information system network documentation.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization implements automated processes to revoke access permissions that are initiated by the termination.

Impact Level Allocation

Low: SG.PS-4	Moderate: SG.PS-4	High: SG.PS-4
--------------	-------------------	---------------

SG.PS-5 Personnel Transfer

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

- 1. The organization reviews logical and physical access permissions to Smart Grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions; and
- 2. Complete execution of this requirement occurs within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources.

Supplemental Guidance

Appropriate actions may include:

- 1. Returning old and issuing new keys, identification cards, and building passes;
- 2. Closing old accounts and establishing new accounts;
- 3. Changing Smart Grid information system access authorizations; and
- 4. Providing access to official records created or managed by the employee at the former work location and in the former accounts.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-5	Moderate: SG.PS-5	High: SG.PS-5
--------------	-------------------	---------------

SG.PS-6 Access Agreements

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization -

1. Completes appropriate agreements for Smart Grid information system access before access is granted. This requirement applies to all parties, including third parties and contractors, who require access to the Smart Grid information system;
2. Reviews and updates access agreements periodically; and
3. Ensures that signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with the Smart Grid information system to which access is authorized.

Supplemental Guidance

Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-6	Moderate: SG.PS-6	High: SG.PS-6
--------------	-------------------	---------------

SG.PS-7 Contractor and Third-Party Personnel Security

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization enforces security requirements for contractor and third-party personnel and monitors service provider behavior and compliance.

Supplemental Guidance

Contactors and third-party providers include service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-7	Moderate: SG.PS-7	High: SG.PS-7
--------------	-------------------	---------------

SG.PS-8 Personnel Accountability

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Victoria Pillitteri 12/4/12 2:45 PM
Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 2:45 PM
Deleted: The organization c

Victoria Pillitteri 12/4/12 2:45 PM
Deleted: The organization r

Victoria Pillitteri 12/4/12 2:45 PM
Deleted: s

Victoria Pillitteri 12/4/12 2:46 PM
Comment [18]: Should check for consistency of use of this term (hyphenated or not) throughout doc (I recall a case in Vuln Classes that isn't hyphenated)

Requirement

The organization -

1. Employs a formal accountability process for personnel failing to comply with established security policies and procedures and identifies disciplinary actions for failing to comply; and
2. Ensures that the accountability process complies with applicable federal, state, local, tribal, and territorial laws and regulations.

Victoria Pillitteri 12/4/12 2:46 PM
Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 2:46 PM
Deleted: The organization e

Victoria Pillitteri 12/4/12 2:46 PM
Deleted: The organization e

Supplemental Guidance

The accountability process can be included as part of the organization’s general personnel policies and procedures.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.PS-8	Moderate: SG.PS-8	High: SG.PS-8
--------------	-------------------	---------------

SG.PS-9 Personnel Roles

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization provides employees, contractors, and third parties with expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. Employees and contractors acknowledge understanding by signature.

Impact Level Allocation

Low: SG.PS-9	Moderate: SG.PS-9	High: SG.PS-9
--------------	-------------------	---------------

3.22 RISK MANAGEMENT AND ASSESSMENT (SG.RA)

Risk management planning is a key aspect of ensuring that the processes and technical means of securing Smart Grid information systems have fully addressed the risks and vulnerabilities in the Smart Grid information system.

An organization identifies and classifies risks to develop appropriate security measures. Risk identification and classification involves security assessments of Smart Grid information systems and interconnections to identify critical components and any areas weak in security. The risk identification and classification process is continually performed to monitor the Smart Grid information system's compliance status.

SG.RA-1 Risk Assessment Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented risk assessment security policy that addresses—
 - i. The objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and
 - ii. The scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the risk assessment policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The risk assessment policy also takes into account the organization's risk tolerance level. The risk assessment policy can be included as part of the general security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular Smart Grid information system, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-1	Moderate: SG.RA-1	High: SG.RA-1
--------------	-------------------	---------------

SG.RA-2 Risk Management Plan

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops a risk management plan;

2. A management authority reviews and approves the risk management plan; and
3. Risk-reduction mitigation measures are planned and implemented and the results monitored to ensure effectiveness of the organization’s risk management plan.

Supplemental Guidance

Risk mitigation measures need to be implemented and the results monitored against planned metrics to ensure the effectiveness of the risk management plan.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-2	Moderate: SG.RA-2	High: SG.RA-2
--------------	-------------------	---------------

SG.RA-3 Security Impact Level

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Specifies the information and the information system impact levels;
2. Documents the impact level results (including supporting rationale) in the security plan for the information system; and
3. Reviews the Smart Grid information system and information impact levels on an organization-defined frequency.

Supplemental Guidance

Impact level designation is based on the need, priority, and level of protection required commensurate with sensitivity and impact of the loss of availability, integrity, or confidentiality. Impact level designation may also be based on regulatory requirements, for example, the NERC CIPs. The organization considers safety issues in determining the impact level for the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-3	Moderate: SG.RA-3	High: SG.RA-3
--------------	-------------------	---------------

SG.RA-4 Risk Assessment

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

- 1. Conducts assessments of risk from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and Smart Grid information systems; and
- 2. Updates risk assessments on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system or environment of operation, or other conditions that may impact the security of the Smart Grid information system.

Supplemental Guidance

Risk assessments take into account vulnerabilities, threat sources, risk tolerance levels, and security mechanisms planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-4	Moderate: SG.RA-4	High: SG.RA-4
--------------	-------------------	---------------

SG.RA-5 Risk Assessment Update

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization updates the risk assessment plan on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system, the facilities where the Smart Grid information system resides, or other conditions that may affect the security or authorization-to-operate status of the Smart Grid information system.

Supplemental Guidance

The organization develops and documents specific criteria for what are considered significant changes to the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.RA-5	Moderate: SG.RA-5	High: SG.RA-5
--------------	-------------------	---------------

SG.RA-6 Vulnerability Assessment and Awareness

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

- 1.** Monitors and evaluates the Smart Grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a Smart Grid information system;
- 2.** Analyzes vulnerability scan reports and remediates vulnerabilities within an organization-defined time frame based on an assessment of risk;
- 3.** Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other Smart Grid information systems;
- 4.** Updates the Smart Grid information system to address any identified vulnerabilities in accordance with organization's Smart Grid information system maintenance policy; and
- 5.** Updates the list of Smart Grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported.

Supplemental Guidance

Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools to scan for Web-based vulnerabilities, source code reviews, and static analysis of source code). Vulnerability scanning includes scanning for ports, protocols, and services that should not be accessible to users and for improperly configured or incorrectly operating information flow mechanisms.

Requirement Enhancements

- 1.** The organization employs vulnerability scanning tools that include the capability to update the list of Smart Grid information system vulnerabilities scanned; and
- 2.** The organization includes privileged access authorization to organization-defined Smart Grid information system components for selected vulnerability scanning activities to facilitate more thorough scanning.

Additional Considerations

- A1.** The organization employs automated mechanisms on an organization-defined frequency to detect the presence of unauthorized software on organizational Smart Grid information systems and notifies designated organizational officials;
- A2.** The organization performs security testing to determine the level of difficulty in circumventing the security requirements of the Smart Grid information system; and
- A3.** The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in Smart Grid information system vulnerabilities.

Impact Level Allocation

Low: SG.RA-6

Moderate: SG.RA-6 (1)

High: SG.RA-6 (1), (2)

3.23 SMART GRID INFORMATION SYSTEM AND SERVICES ACQUISITION (SG.SA)

Smart Grid information systems and services acquisition covers the contracting and acquiring of system components, software, firmware, and services from employees, contactors, and third parties. A policy with detailed procedures for reviewing acquisitions should reduce the introduction of additional or unknown vulnerabilities into the Smart Grid information system.

SG.SA-1 Smart Grid Information System and Services Acquisition Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

- 1.** The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented Smart Grid information system and services acquisition security policy that addresses—
 - i. The objectives, roles, and responsibilities for the Smart Grid information system and services acquisition security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the Smart Grid information system and services acquisition security program as it applies to all of the organizational staff, contactors, and third parties; and
 - b. Procedures to address the implementation of the Smart Grid information system and services acquisition policy and associated physical and environmental protection requirements;
- 2.** Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
- 3.** The organization ensures that the Smart Grid information system and services acquisition policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The Smart Grid information system and services acquisition policy can be included as part of the general information security policy for the organization. Smart Grid information system and services acquisition procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-1	Moderate: SG.SA-1	High: SG.SA-1
--------------	-------------------	---------------

SG.SA-2 Security Policies for Contractors and Third Parties

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization -

1. Ensures external suppliers and contractors that have an impact on the security of Smart Grid information systems must meet the organization's policy and procedures; and
2. Establishes procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the contract.

Supplemental Guidance

The organization considers the increased security risk associated with outsourcing as part of the decision-making process to determine what to outsource and what outsourcing partner to select. Contracts with external suppliers govern physical as well as logical access. The organization considers confidentiality or nondisclosure agreements and intellectual property rights.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-2	Moderate: SG.SA-2	High: SG.SA-2
--------------	-------------------	---------------

SG.SA-3 Life-Cycle Support

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization manages the Smart Grid information system using a system development lifecycle methodology that includes security.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Victoria Pillitteri 12/4/12 2:48 PM
Formatted: No bullets or numbering

Victoria Pillitteri 12/4/12 2:49 PM
Deleted: E

Victoria Pillitteri 12/4/12 2:49 PM
Deleted: The organization e

Low: SG.SA-3	Moderate: SG.SA-3	High: SG.SA-3
--------------	-------------------	---------------

SG.SA-4 Acquisitions

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization includes security requirements in Smart Grid information system acquisition contracts in accordance with applicable laws, regulations, and organization-defined security policies.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-4	Moderate: SG.SA-4	High: SG.SA-4
--------------	-------------------	---------------

SG.SA-5 Smart Grid Information System Documentation

Category: Common Governance, Risk, and Compliance (GRC) Requirement

Requirement

1. Smart Grid information system documentation includes how to configure, install, and use the Smart Grid information system and the it's security features; and
2. The organization obtains from the contractor/third-party, information describing the functional properties of the security controls employed within the Smart Grid information system.

Victoria Pillitteri 12/4/12 2:49 PM
Deleted: information system's

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-5	Moderate: SG.SA-5	High: SG.SA-5
--------------	-------------------	---------------

SG.SA-6 Software License Usage Restrictions

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

1. Uses software and associated documentation in accordance with contract agreements and copyright laws; and
2. Controls the use of software and associated documentation protected by quantity licenses and copyrighted material.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-6	Moderate: SG.SA-6	High: SG.SA-6
--------------	-------------------	---------------

SG.SA-7 User-Installed Software

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization establishes policies and procedures to manage user installation of software.

Supplemental Guidance

If provided the necessary privileges, users have the ability to install software. The organization's security program identifies the types of software permitted to be downloaded and installed (e.g., updates and security patches to existing software) and types of software prohibited (e.g., software that is free only for personal, not corporate use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-7	Moderate: SG.SA-7	High: SG.SA-7
--------------	-------------------	---------------

SG.SA-8 Security Engineering Principles

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization applies security engineering principles in the specification, design, development, and implementation of any Smart Grid information system.

Security engineering principles include:

1. Ongoing secure development education requirements for all developers involved in the Smart Grid information system;
2. Specification of a minimum standard for security;
3. Specification of a minimum standard for privacy;
4. Creation of a threat model for a Smart Grid information system;
5. Updating of product specifications to include mitigations for threats discovered during threat modeling;
6. Use of secure coding practices to reduce common security errors;
7. Testing to validate the effectiveness of secure coding practices;
8. Performance of a final security audit prior to authorization to operate to confirm adherence to security requirements;
9. Creation of a documented and tested security response plan in the event vulnerability is discovered;
10. Creation of a documented and tested privacy response plan in the event vulnerability is discovered; and
11. Performance of a root cause analysis to understand the cause of identified vulnerabilities.

Supplemental Guidance

The application of security engineering principles is primarily targeted at new development Smart Grid information systems or Smart Grid information systems undergoing major upgrades. These principles are integrated into the Smart Grid information system development life cycle. For legacy Smart Grid information systems, the organization applies security engineering principles to Smart Grid information system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the Smart Grid information system. The organization minimizes risk to legacy systems through attack surface reduction and other mitigating controls.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SA-8	Moderate: SG.SA-8	High: SG.SA-8
--------------	-------------------	---------------

SG.SA-9 Developer Configuration Management

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization requires that Smart Grid information system developers/integrators document and implement a configuration management process that—

- 1. Manages and controls changes to the Smart Grid information system during design, development, implementation, and operation;
- 2. Tracks security flaws; and
- 3. Includes organizational approval of changes.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

A1. The organization requires that Smart Grid information system developers/integrators provide an integrity check of delivered software and firmware.

Impact Level Allocation

Low: SG.SA-9	Moderate: SG.SA-9	High: SG.SA-9
--------------	-------------------	---------------

SG.SA-10 Developer Security Testing

Category: ~~Common Governance, Risk, and Compliance (GRC) Requirements~~, Integrity

Requirement

- 1. The Smart Grid information system developer creates a security test and evaluation plan;
- 2. The developer submits the plan to the organization for approval and implements the plan once written approval is obtained;
- 3. The developer documents the results of the testing and evaluation and submits them to the organization for approval; and
- 4. The organization does not perform developmental security tests on the production Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

Victoria Pillitteri 12/4/12 2:50 PM
Deleted: Common Technical Requirements

- A1. The organization requires that Smart Grid information system developers employ code analysis tools to examine software for common flaws and document the results of the analysis; and
- A2. The organization requires that Smart Grid information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.

Impact Level Allocation

Low: SG.SA-10	Moderate: SG.SA-10	High: SG.SA-10
---------------	--------------------	----------------

SG.SA-11 Supply Chain Protection

Category: Common Governance, Risk, and Compliance (GRC) Requirements, Integrity

Requirement

The organization protects against supply chain vulnerabilities employing requirements defined to protect the products and services from threats initiated against organizations, people, information, and resources, possibly international in scope, that provides products or services to the organization.

Supplemental Guidance

Supply chain protection helps to protect Smart Grid information systems (including the technology products that compose those Smart Grid information systems) throughout the system development life cycle (e.g., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement).

Requirement Enhancements

None.

Additional Considerations

- A1. The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire Smart Grid information system hardware, software, firmware, or services;
- A2. The organization uses a diverse set of suppliers for Smart Grid information systems, Smart Grid information system components, technology products, and Smart Grid information system services; and
- A3. The organization employs independent analysis and penetration testing against delivered Smart Grid information systems, Smart Grid information system components, and technology products.

Impact Level Allocation

Low: SG.SA-11	Moderate: SG.SA-11	High: SG.SA-11
---------------	--------------------	----------------

Victoria Pillitteri 12/4/12 2:50 PM
 Deleted: Common Technical Requirements

3.24 SMART GRID INFORMATION SYSTEM AND COMMUNICATION PROTECTION (SG.SC)

Smart Grid information system and communication protection consists of steps taken to protect the Smart Grid information system and the communication links between Smart Grid information system components from cyber intrusions. Although Smart Grid information system and communication protection might include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in SG.PE, Physical and Environmental Security.

SG.SC-1 Smart Grid Information System and Communication Protection Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented Smart Grid information system and communication protection security policy that addresses—
 - i. The objectives, roles, and responsibilities for the Smart Grid information system and communication protection security program as it relates to protecting the organization's personnel and assets; and
 - ii. The scope of the Smart Grid information system and communication protection policy as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the Smart Grid information system and communication protection security policy and associated Smart Grid information system and communication protection requirements;
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the Smart Grid information system and communication protection policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The Smart Grid information system and communication protection policy may be included as part of the general information security policy for the organization. Smart Grid information system and communication protection procedures can be developed for the security program in general and a Smart Grid information system in particular, when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-1	Moderate: SG.SC-1	High: SG.SC-1
--------------	-------------------	---------------

SG.SC-2 Communications Partitioning

Category: Unique Technical Requirements

Requirement

The Smart Grid information system partitions the communications for telemetry/data acquisition services and management functionality.

Supplemental Guidance

The Smart Grid information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-3 Security Function Isolation

Category: Unique Technical Requirements

Requirement

The Smart Grid information system isolates security functions from nonsecurity functions.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system employs underlying hardware separation mechanisms to facilitate security function isolation; and
- A2. The Smart Grid information system isolates security functions (e.g., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.

Impact Level Allocation

Low: SG.SC-3	Moderate: SG.SC-3	High: SG.SC-3
--------------	-------------------	---------------

SG.SC-4 Information Remnants

Category: Unique Technical Requirements

Requirement

The Smart Grid information system prevents unauthorized or unintended information transfer via shared Smart Grid information system resources.

Supplemental Guidance

Control of Smart Grid information system remnants, sometimes referred to as object reuse, or data remnants, prevents information from being available to any current user/role/process that obtains access to a shared Smart Grid information system resource after that resource has been released back to the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-4	High: SG.SC-4
-------------------	-------------------	---------------

SG.SC-5 Denial-of-Service Protection

Category: Unique Technical Requirements

Requirement

The Smart Grid information system mitigates or limits the effects of denial-of-service attacks based on an organization-defined list of denial-of-service attacks.

Supplemental Guidance

Network perimeter devices can filter certain types of packets to protect devices on an organization’s internal network from being directly affected by denial-of-service attacks.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system restricts the ability of users to launch denial-of-service attacks against other Smart Grid information systems or networks; and
- A2. The Smart Grid information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

Impact Level Allocation

Low: SG.SC-5	Moderate: SG.SC-5	High: SG.SC-5
--------------	-------------------	---------------

SG.SC-6 Resource Priority

Category: Unique Technical Requirements

Requirement

The Smart Grid information system prioritizes the use of resources.

Supplemental Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the Smart Grid information system servicing any higher-priority process. This requirement does not apply to components in the Smart Grid information system for which only a single user/role exists.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-7 Boundary Protection

Category: Unique Technical Requirements

Requirement

1. The organization defines the boundary of the Smart Grid information system;
2. The Smart Grid information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
3. The Smart Grid information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices;
4. The managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information; and
5. The organization prevents public access into the organization's internal Smart Grid information system networks except as appropriately mediated.

Supplemental Guidance

Managed interfaces employing boundary protection devices include proxies, gateways, routers, firewalls, guards, or encrypted tunnels.

Requirement Enhancements

1. The Smart Grid information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception);
2. The Smart Grid information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination; and

- 3. Communications to/from Smart Grid information system components shall be restricted to specific components in the Smart Grid information system. Communications shall not be permitted to/from any non-Smart Grid system unless separated by a controlled logical/physical interface.

Additional Considerations

- A1. The organization prevents the unauthorized release of information outside the Smart Grid information system boundary or any unauthorized communication through the Smart Grid information system boundary when an operational failure occurs of the boundary protection mechanisms;
- A2. The organization prevents the unauthorized exfiltration of information across managed interfaces;
- A3. The Smart Grid information system routes internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices;
- A4. The organization limits the number of access points to the Smart Grid information system to allow for better monitoring of inbound and outbound network traffic;
- A5. Smart Grid information system boundary protections at any designated alternate processing/control sites provide the same levels of protection as that of the primary site; and
- A6. The Smart Grid information system fails securely in the event of an operational failure of a boundary protection device.

Impact Level Allocation

Low: SG.SC-7	Moderate: SG.SC-7 (1), (2), (3)	High: SG.SC-7 (1), (2), (3)
--------------	---------------------------------	-----------------------------

SG.SC-8 Communication Integrity

Category: Unique Technical Requirements, Integrity

Requirement

The Smart Grid information system protects the integrity of electronically communicated information.

Supplemental Guidance

It is feasible to implement this requirement at one or more various locations within the communications stack; each placement location carries varying benefits and downsides.

Victoria Pillitteri 12/4/12 2:54 PM
Deleted: None.

Requirement Enhancements

- 1. The organization employs cryptographic mechanisms to ensure integrity.

Additional Considerations

- A1. The Smart Grid information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-8 (1)	High: SG.SC-8 (1)
-------------------	-----------------------	-------------------

SG.SC-9 Communication Confidentiality

Category: Unique Technical Requirements, [Confidentiality](#)

Requirement

The Smart Grid information system protects the confidentiality of communicated information.

Supplemental Guidance

[It is feasible to implement this requirement at one or more various locations within the communications stack; each placement location carries varying benefits and downsides.](#)

Requirement Enhancements

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-9 (1)	High: SG.SC-9 (1)
-------------------	-----------------------	-------------------

SG.SC-10 Trusted Path

Category: Unique Technical Requirements

Requirement

The Smart Grid information system establishes a trusted communications path between the user and the Smart Grid information system.

Supplemental Guidance

A trusted path is the means by which a user and target of evaluation security functionality can communicate with the necessary confidence.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-11 Cryptographic Key Establishment and Management

Category: Common Technical Requirements, Confidentiality

Requirement

Victoria Pillitteri 12/4/12 2:55 PM

Deleted: None.

The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance

Key establishment includes a key generation process in accordance with a specified algorithm and key sizes, and key sizes based on an assigned standard. Key generation must be performed using an appropriate random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution.

Requirement Enhancements

1. The organization maintains availability of information in the event of the loss of cryptographic keys by users. *See* Chapter 4 for key management requirements.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-11	Moderate: SG.SC-11 (1)	High: SG.SC-11 (1)
---------------	------------------------	--------------------

SG.SC-12 Use of **FIPS** Cryptography

Category: Common Technical Requirements, Confidentiality

Requirement

All of the cryptography and other security functions (e.g., hashes, random number generators, etc.) that are required for use in a Smart Grid information system shall be NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes.

Supplemental Guidance

For a list of current FIPS-approved or allowed cryptography, *see* [Chapter Four Cryptography and Key Management](#).

Requirement Enhancements

None.

Additional Considerations

- A1. **The organization ensures that vendors have validated or demonstrated conformance of their cryptographic modules and other security functions.**

Impact Level Allocation

Low: SG.SC-12	Moderate: SG.SC-12	High: SG.SC-12
---------------	--------------------	----------------

SG.SC-13 Collaborative Computing

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization develops, disseminates, and periodically reviews and updates on an organization-defined frequency a collaborative computing policy.

Victoria Pillitteri 12/4/12 2:55 PM
Deleted: Validated

Victoria Pillitteri 1/3/13 1:04 PM
Formatted: Default Paragraph Font

Victoria Pillitteri 11/20/12 3:11 PM
Deleted: Chapter Four
Cryptography and Key Management

Victoria Pillitteri 12/4/12 2:56 PM
Deleted: None.

Supplemental Guidance

Collaborative computing mechanisms include video and audio conferencing capabilities or instant messaging technologies. Explicit indication of use includes signals to local users when cameras and/or microphones are activated.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-13	Moderate: SG.SC-13	High: SG.SC-13
---------------	--------------------	----------------

SG.SC-14 Transmission of Security Parameters

Category: Unique Technical Requirements

Requirement

The Smart Grid information system reliably associates security parameters with information exchanged between the enterprise information systems and the Smart Grid information system.

Supplemental Guidance

Security parameters may be explicitly or implicitly associated with the information contained within the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system validates the integrity of security parameters exchanged between Smart Grid information systems.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-15 Public Key Infrastructure Certificates

Category: Common Technical Requirements, Confidentiality

Requirement

For Smart Grid information systems that implement a public key infrastructure, the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-15	Moderate: SG.SC-15	High: SG.SC-15
---------------	--------------------	----------------

SG.SC-16 Mobile Code

Category: Common Technical Requirements, Confidentiality

Requirement

The organization—

1. Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the Smart Grid information system if used maliciously;
2. Documents, monitors, and manages the use of mobile code within the Smart Grid information system; and
3. A management authority authorizes the use of mobile code.

Supplemental Guidance

Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance need to apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-16	High: SG.SC-16
-------------------	--------------------	----------------

SG.SC-17 Voice-Over Internet Protocol

Category: Unique Technical Requirements, [Availability](#)

Requirement

The organization—

1. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the Smart Grid information system.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-17	High: SG.SC-17
-------------------	--------------------	----------------

SG.SC-18 System Connections

Category: Common Technical Requirements, Integrity

Requirement

All external Smart Grid information system and communication connections are identified and protected from tampering or damage.

Supplemental Guidance

The intent of this requirement is to address end-to-end connection integrity. For example, external access point connections to the Smart Grid information system need to be secured to protect the Smart Grid information system. Access points include any externally connected communication end point (for example, dial-up modems). This requirement applies to dedicated connections between Smart Grid information systems and does not apply to transitory, user-controlled connections.

Requirement Enhancements

None.

Additional Considerations

A1. Logical connections are monitored for changes in configured or remote endpoints, when technically feasible.

Impact Level Allocation

Low: SG.SC-18	Moderate: SG.SC-18	High: SG.SC-18
---------------	--------------------	----------------

SG.SC-19 Security Roles

Category: Common Governance, Risk, and Compliance (GRC) Requirements, Integrity

Victoria Pillitteri 12/4/12 2:58 PM
Deleted: Confidentiality

Victoria Pillitteri 12/4/12 2:58 PM
Deleted: E

Victoria Pillitteri 12/4/12 2:59 PM
Deleted: None.

Victoria Pillitteri 12/4/12 3:00 PM
Deleted: Common Technical Requirements

Requirement

The Smart Grid information system design and implementation specifies the security roles and responsibilities for the users of the Smart Grid information system.

Supplemental Guidance

Security roles and responsibilities for Smart Grid information system users need to be specified, defined, and implemented based on the sensitivity of the information handled by the user. These roles may be defined for specific job descriptions or for individuals.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-19	Moderate: SG.SC-19	High: SG.SC-19
---------------	--------------------	----------------

SG.SC-20 Message Authenticity

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system provides mechanisms to protect the authenticity of device-to-device communications.

Supplemental Guidance

Message authentication provides protection from malformed traffic, misconfigured devices, and malicious entities.

Requirement Enhancements

None.

Additional Considerations

- A1. Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.

Impact Level Allocation

Low: SG.SC-20	Moderate: SG.SC-20	High: SG.SC-20
---------------	--------------------	----------------

SG.SC-21 Secure Name/Address Resolution Service

Category: Common Technical Requirements, Integrity

Requirement

The organization is responsible for—

1. Configuring systems that provide name/address resolution to supply additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries; and
2. Configuring systems that provide name/address resolution to Smart Grid information systems, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SC-21	Moderate: SG.SC-21	High: SG.SC-21
---------------	--------------------	----------------

SG.SC-22 Fail in Known State

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system fails to a known state for defined failures.

Supplemental Guidance

Failure in a known state can be interpreted by organizations in the context of safety or security in accordance with the organization’s mission/business/operational needs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the Smart Grid information system or a component of the Smart Grid information system.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system preserves defined system state information in failure.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-22	High: SG.SC-22
-------------------	--------------------	----------------

SG.SC-23 Thin Nodes

Category: Unique Technical Requirements

Requirement

The Smart Grid information system employs processing components that have minimal functionality and data storage.

Supplemental Guidance

The deployment of Smart Grid information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the number of endpoints to be secured and may reduce the exposure of information, Smart Grid information systems, and services to a successful attack.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-24 Honey pots

Category: Unique Technical Requirements

Requirement

The Smart Grid information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system includes components that proactively seek to identify Web-based malicious code.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-25 Operating System-Independent Applications

Category: Unique Technical Requirements

Requirement

The Smart Grid information system includes organization-defined applications that are independent of the operating system.

Supplemental Guidance

Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, thus increasing the availability for critical functionality while an organization is under an attack exploiting vulnerabilities in a given operating system.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-26 Confidentiality of Information at Rest

Category: Unique Technical Requirements

Requirement

The Smart Grid information system employs cryptographic mechanisms for all critical security parameters (e.g., cryptographic keys, passwords, security configurations) to prevent unauthorized disclosure of information at rest.

Supplemental Guidance

[Refer to SG.SC-12 for additional information.](#)

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-26	High: SG.SC-26
-------------------	--------------------	----------------

SG.SC-27 Heterogeneity

Category: Unique Technical Requirements

Requirement

The organization employs diverse technologies in the implementation of the Smart Grid information system.

Supplemental Guidance

Increasing the diversity of technologies within the Smart Grid information system reduces the impact from the exploitation of a specific technology.

Requirement Enhancements

None.

Victoria Pillitteri 12/4/12 3:02 PM
Deleted: For a list of current FIPS-approved or allowed cryptography, see Chapter Four - Cryptography and Key Management

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-28 Virtualization Techniques

Category: Unique Technical Requirements

Requirement

The organization employs virtualization techniques to present gateway components into Smart Grid information system environments as other types of components, or components with differing configurations.

Supplemental Guidance

Virtualization techniques provide organizations with the ability to disguise gateway components into Smart Grid information system environments, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications;
- A2. The organization changes the diversity of operating systems and applications on an organization-defined frequency; and
- A3. The organization employs randomness in the implementation of the virtualization.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: Not Selected
-------------------	------------------------	--------------------

SG.SC-29 Application Partitioning

Category: Unique Technical Requirements

Requirement

The Smart Grid information system separates user functionality (including user interface services) from Smart Grid information system management functionality.

Supplemental Guidance

Smart Grid information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from Smart Grid information system management functionality is either physical or logical.

Requirement Enhancements

None.

Additional Considerations

A1. The Smart Grid information system prevents the presentation of Smart Grid information system management-related functionality at an interface for general (i.e., non-privileged) users.

Additional Considerations Supplemental Guidance

The intent of this additional consideration is to ensure that administration options are not available to general users. For example, administration options are not presented until the user has appropriately established a session with administrator privileges.

Impact Level Allocation

Low: Not Selected	Moderate: Not Selected	High: SG.SC-29
-------------------	------------------------	----------------

SG.SC-30 Smart Grid Information System Partitioning

Category: Common Technical Requirements, Integrity

Requirement

The organization partitions the Smart Grid information system into components residing in separate physical or logical domains (or environments).

Supplemental Guidance

An organizational assessment of risk guides the partitioning of Smart Grid information system components into separate domains (or environments).

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SC-30	High: SG.SC-30
-------------------	--------------------	----------------

3.25 SMART GRID INFORMATION SYSTEM AND INFORMATION INTEGRITY (SG.SI)

Maintaining a Smart Grid information system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security requirements described under the Smart Grid information system and information integrity family provide policy and procedure for identifying, reporting, and correcting Smart Grid information system flaws. Requirements exist for malicious code detection. Also provided are requirements for receiving security alerts and advisories and the verification of security functions on the Smart Grid information system. In addition, requirements within this family detect and protect against unauthorized changes to software and

data; restrict data input and output; check the accuracy, completeness, and validity of data; and handle error conditions.

SG.SI-1 Smart Grid Information System and Information Integrity Policy and Procedures

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
 - a. A documented Smart Grid information system and information integrity security policy that addresses—
 - i. The objectives, roles, and responsibilities for the Smart Grid information system and information integrity security program as it relates to protecting the organization’s personnel and assets; and
 - ii. The scope of the Smart Grid information system and information integrity security program as it applies to all of the organizational staff, contractors, and third parties; and
 - b. Procedures to address the implementation of the Smart Grid information system and information integrity security policy and associated Smart Grid information system and information integrity protection requirements;
2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and
3. The organization ensures that the Smart Grid information system and information integrity policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

Supplemental Guidance

The Smart Grid information system and information integrity policy can be included as part of the general control security policy for the organization. Smart Grid information system and information integrity procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SI-1	Moderate: SG.SI-1	High: SG.SI-1
--------------	-------------------	---------------

SG.SI-2 Flaw Remediation

Category: Common Technical Requirements, Integrity

Requirement

The organization—

1. Identifies, reports, and corrects Smart Grid information system flaws;
2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational Smart Grid information systems before installation; and
3. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance

The organization identifies Smart Grid information systems containing software and firmware (including operating system software) affected by recently announced flaws (and potential vulnerabilities resulting from those flaws). Flaws discovered during security assessments, continuous monitoring, or under incident response activities also need to be addressed.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization centrally manages the flaw remediation process. Organizations consider the risk of employing automated flaw remediation processes on a Smart Grid information system;
- A2. The organization employs automated mechanisms on an organization-defined frequency and on demand to determine the state of Smart Grid information system components with regard to flaw remediation; and
- A3. The organization employs automated patch management tools to facilitate flaw remediation to organization-defined Smart Grid information system components.

Impact Level Allocation

Low: SG.SI-2	Moderate: SG.SI-2	High: SG.SI-2
--------------	-------------------	---------------

SG.SI-3 Malicious Code and Spam Protection

Category: ~~Common Technical~~ Requirements

Requirement

1. The organization—
 - a. Implements malicious code protection mechanisms; and
 - b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; and
2. The Smart Grid information system prevents users from circumventing malicious code protection capabilities.

Supplemental Guidance

None.

Victoria Pillitteri 12/4/12 3:02 PM
Deleted: Common Governance, Risk, and Compliance (GRC)

Requirement Enhancements

None.

Additional Considerations

- A1. The organization centrally manages malicious code protection mechanisms;
- A2. The Smart Grid information system updates malicious code protection mechanisms in accordance with organization-defined policies and procedures;
- A3. The organization configures malicious code protection methods to perform periodic scans of the Smart Grid information system on an organization-defined frequency;
- A4. The use of mechanisms to centrally manage malicious code protection must not degrade the operational performance of the Smart Grid information system; and
- A5. The organization employs spam protection mechanisms at system entry points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, or other common means.

Impact Level Allocation

Low: SG.SI-3	Moderate: SG.SI-3	High: SG.SI-3
--------------	-------------------	---------------

SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques

Category: Common Technical Requirements

Requirement

The organization monitors events on the Smart Grid information system to detect attacks, unauthorized activities or conditions, and non-malicious errors.

Supplemental Guidance

Smart Grid information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, and network forensic analysis tools). The granularity of the information collected can be determined by the organization based on its monitoring objectives and the capability of the Smart Grid information system to support such activities.

Requirement Enhancements

None.

Additional Considerations

- A1. The Smart Grid information system notifies a defined list of incident response personnel;
- A2. The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion;
- A3. The organization tests/exercises intrusion monitoring tools on a defined time period;

Victoria Pillitteri 12/4/12 3:03 PM

Deleted: Governance, Risk, and Compliance (GRC)

- A4. The organization interconnects and configures individual intrusion detection tools into a Smart Grid system-wide intrusion detection system using common protocols;
- A5. The Smart Grid information system provides a real-time alert when indications of compromise or potential compromise occur; and
- A6. The Smart Grid information system prevents users from circumventing host-based intrusion detection and prevention capabilities.

Impact Level Allocation

Low: SG.SI-4	Moderate: SG.SI-4	High: SG.SI-4
--------------	-------------------	---------------

SG.SI-5 Security Alerts and Advisories

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

The organization—

- 1. Receives Smart Grid information system security alerts, advisories, and directives from external organizations; and
- 2. Generates and disseminates internal security alerts, advisories, and directives as deemed necessary.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs automated mechanisms to disseminate security alert and advisory information throughout the organization.

Impact Level Allocation

Low: SG.SI-5	Moderate: SG.SI-5	High: SG.SI-5
--------------	-------------------	---------------

SG.SI-6 Security Functionality Verification

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement

- 1. The organization verifies the correct operation of security functions within the Smart Grid information system upon—
 - a. Smart Grid information system startup and restart; and
 - b. Command by user with appropriate privilege at an organization-defined frequency; and

2. The Smart Grid information system notifies the management authority when anomalies are discovered.

Supplemental Guidance

None.

Requirement Enhancements

None.

Additional Considerations

- A1. The organization employs automated mechanisms to provide notification of failed automated security tests; and
- A2. The organization employs automated mechanisms to support management of distributed security testing.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SI-6	High: SG.SI-6
-------------------	-------------------	---------------

SG.SI-7 Software and Information Integrity

Category: Unique Technical Requirements

Requirement

The Smart Grid information system monitors and detects unauthorized changes to software and information.

Supplemental Guidance

The organization employs integrity verification techniques on the Smart Grid information system to look for evidence of information tampering, errors, and/or omissions.

Requirement Enhancements

1. The organization reassesses the integrity of software and information by performing on an organization-defined frequency integrity scans of the Smart Grid information system.

Additional Considerations

- A1. The organization employs centrally managed integrity verification tools; and
- A2. The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SI-7 (1)	High: SG.SI-7 (1)
-------------------	-----------------------	-------------------

SG.SI-8 Information Input Validation

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system employs mechanisms to check information for accuracy, completeness, validity, and authenticity.

Supplemental Guidance

Rules for checking the valid syntax of Smart Grid information system input (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: Not Selected	Moderate: SG.SI-8	High: SG.SI-8
-------------------	-------------------	---------------

SG.SI-9 Error Handling

Category: Common Technical Requirements, Integrity

Requirement

The Smart Grid information system—

1. Identifies error conditions; and
2. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries.

Supplemental Guidance

The extent to which the Smart Grid information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Requirement Enhancements

None.

Additional Considerations

None.

Impact Level Allocation

Low: SG.SI-9	Moderate: SG.SI-9	High: SG.SI-9
--------------	-------------------	---------------

3.26 TESTING AND CERTIFICATION OF SMART GRID CYBER SECURITY

The testing and certification of the Smart Grid cybersecurity requirements provide assurance that systems and system components are conformant to the requirements selected by the organization. The use of consistent, standardized cybersecurity evaluation criteria and methodologies contributes to the repeatability and objectivity of test results, which provide insight into the extent to which the requirements are implemented correctly, operating as intended, and producing the desired security posture for the Smart Grid information system and system

Victoria Pillitteri 12/4/12 3:04 PM
Deleted: <#> - ... [2]

Victoria Pillitteri 12/4/12 3:08 PM
Formatted: Heading 2,h2, Indent: Left: 0", Hanging: 0.5"

components. Understanding the overall effectiveness of the security requirements implemented in the Smart Grid information system and its operational environment is essential in determining the risk to the organization's operations.

*Guide for Assessing the High-Level Security Requirements in NISTIR 7628*²² (*The 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. *The Guide* is written to provide a foundation to facilitate a security assessment based on the high-level security requirements identified earlier in this chapter, implemented within an effective risk management program. It includes descriptions of the basic concepts needed when assessing the high-level security requirements in Smart Grid information systems, the Security Assessment process (including specific activities carried out in each phase of the assessment), the assessment method definitions, the Assessment Procedures Catalog and a Sample Security Assessment Report outline. Additionally, the Assessment Procedures Catalog has been placed in a companion spreadsheet tool²³ for assessors that can be used to record the findings of an assessment and used as the basis for the development of a final assessment report.

The objective of security assessments is to verify that the implementers and operators of Smart Grid information systems are meeting their stated goals. The security assessment process involves participation and buy-in from both the assessor and organizational stakeholders. Key organizational participants in the process include senior management, Smart Grid information system and industrial control system owners, and the Chief Information Security Officer. The result of the security assessment provides realistic information to senior management about the risk posture and residual risks of the Smart Grid information system, which will form the basis for any decision to approve or authorize the system for operation.

However, cybersecurity testing does not operate in a vacuum; these efforts should be performed in coordination with interoperability testing to ensure that changes to one do not adversely impact the operation of the other. For instance, as a functionality is developed to enable interoperability, new potential vulnerabilities can be introduced. By ensuring that cybersecurity testing is coordinated with interoperability testing, design, implementation and operational flaws that could allow the violation of cybersecurity requirements, and loopholes that can cause loss of information, availability, or allow unauthorized access can be identified and mitigated.

The Smart Grid Interoperability Panel (SGIP) Smart Grid Testing and Certification Committee (SGTCC) developed and issued an Interoperability Process Reference Manual (IPRM) Version 2.0²⁴ in January 2012 that details its recommendations on processes and best practices that enhance the introduction of interoperable products in the marketplace. These recommendations build upon international standards-based processes (ISO/IEC 17025 and ISO/IEC Guide 65) for

²² *Guide for Assessing the High-Level Security Requirements in NISTIR 7628* is available for download at: https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/NISTIR_7628_Assessment_Guide-v1p0-24Aug2012.pdf

²³ The Companion Spreadsheet to the Guide for Assessing the High-Level Security Requirements in NISTIR 7628 is available at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/2012-004_1_Companion_Spreadsheet.docx

²⁴ The *IPRM Version 2.0* is available for download at: https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SmartGridTestingAndCertificationCommittee/IPRM_final_-_011612.pdf

interoperability testing and certification for testing laboratories and certification body management systems. Additionally, the IPRM identifies technical requirements and best practices necessary to help assure testing programs' technical depth and sufficiency for interoperability and cybersecurity. The IPRM Version 2.0 includes sections that discuss: International Guidelines for Testing and Certification, ITCA Implementation of the IPRM, Interoperability and Conformance Test Construction, Cybersecurity Testing, and Interoperability Certification Body and Testing Laboratory Requirements.

The SGTCC asserts that implementation of the IPRM by Interoperability Testing and Certification Authorities (ITCAs) will increase the quality of standards-based, secure and interoperable products in the Smart Grid marketplace. Implementation of the IPRM will lead to reduced deployment costs of Smart Grid systems and devices, and enhanced product quality with respect to interoperability and conformance. This will ultimately provide increased end-user customer satisfaction and confidence to the buyer through meaningful certification programs. For instance, as electric utilities turn to Advanced Metering Infrastructures (AMIs) to promote the development and deployment of the Smart Grid, one aspect that can benefit from standardization is the upgradeability of Smart Meters. The National Electrical Manufacturers Association (NEMA) standard SG-AMI 1-2009, "Requirements for Smart Meter Upgradeability," describes functional and security requirements for the secure upgrade—both local and remote—of Smart Meters. Draft NISTIR 7823, *Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework*, describes conformance test requirements that may be used voluntarily by testers and/or test laboratories to determine whether Smart Meters and Upgrade Management Systems conform to the requirements of NEMA SG-AMI 1-2009.

DRAFT

APPENDIX A

CROSSWALK OF CYBER SECURITY DOCUMENTS

Table A-1 Crosswalk of Cyber Security Requirements and Documents

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
Access Control (SG.AC)						
SG.AC-1	Access Control Policy and Procedures	AC-1	Access Control Policy and Procedures	2.15.1	Access Control Policies and Procedures	CIP 003-4 (R1, R2, R3, R5, R5.2, R5.3) CIP 005-4a (R1, R1.1, R1.6) CIP 006-4 (R2)
SG.AC-2	Remote Access Policy and Procedures	AC-17	Remote Access	2.15.23	Remote Access Policy and Procedures	CIP 005-4a (R1, R1.1, R1.2, R1.6, R2, R2.3, R2.4) CIP 007-4 (R5)
SG.AC-3	Account Management	AC-2	Account Management	2.15.3	Account Management	CIP 003-4 (R5, R5.1, R5.2, R5.3) CIP 004-4 (R4, R4.1, R4.2) CIP 005-4a (R2.5.1, R2.5.3) CIP 007-4 (R5, R5.1, R5.1.3, R5.2, R5.2.3)
SG.AC-4	Access Enforcement	AC-3	Access Enforcement	2.15.7	Access Enforcement	CIP 004-4 (R4) CIP 005-4a (R1.6, R2, R2.1-R2.4) CIP 007-4 (R5)

Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺
 Brian Mckay 11/13/12 9:55 PM
 Deleted: May 2009

Brian Mckay 11/13/12 9:55 PM
 Deleted: CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)

Brian Mckay 11/13/12 9:55 PM
 Deleted: CIP005-2 (R1, R1.1, R1.2, R2, R2.3, R2.4)

Brian Mckay 11/13/12 9:55 PM
 Deleted: CIP 003-2 (R5, R5.1, R5.2, R5... [3])

Brian Mckay 11/13/12 9:56 PM
 Deleted: CIP 004-2 (R4) - ... [4]

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.AC-5	Information Flow Enforcement	AC-4	Information Flow Enforcement	2.15.15	Information Flow Enforcement	None
SG.AC-6	Separation of Duties	AC-5	Separation of Duties	2.15.8	Separation of Duties	CIP 005-4a (R2, R2.1) CIP 007-4 (R5.1, R5.2)
SG.AC-7	Least Privilege	AC-6	Least Privilege	2.15.9	Least Privilege	CIP 007-4 (R5.1, R5.2)
SG.AC-8	Unsuccessful Login Attempts	AC-7	Unsuccessful Login Attempts	2.15.20	Unsuccessful Logon Notification	CIP 007-4 (R5)
SG.AC-9	Smart Grid Information System Use Notification	AC-8	System Use Notification	2.15.17	System Use Notification	CIP 005-4a (R2.6)
SG.AC-10	Previous Logon Notification	AC-9	Previous Logon (Access) Notification	2.15.19	Previous Logon Notification	None
SG.AC-11	Concurrent Session Control	AC-10	Concurrent Session Control	2.15.18	Concurrent Session Control	None
SG.AC-12	Session Lock	AC-11	Session Lock	2.15.21	Session Lock	None
SG.AC-13	Remote Session Termination			2.15.22	Remote Session Termination	CIP 007-4 (R6)
SG.AC-14	Permitted Actions without Identification or Authentication	AC-14	Permitted Actions without Identification or Authentication	2.15.11	Permitted Actions without Identification and Authentication	None

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 9:56 PM

Deleted: CIP 007-2 (R5.1)

Brian Mckay 11/13/12 9:57 PM

Deleted: CIP 005-2 (R2.6)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) <u>Version 4</u>
SG.AC-15	Remote Access	AC-17	Remote Access	2.15.24	Remote Access	CIP 005-4a (R2, R2.1-R2.5, R3, R3.1, R3.2) CIP 007-4 (R2.1, R5), Enhancement: CIP 005-4a (R1.2, R2.3, R3, R3.2) CIP 007-4 (R5, R6, R6.2)
SG.AC-16	Wireless Access Restrictions			2.15.26	Wireless Access Restrictions	CIP 005-4a (R1.1, R2, R2.4, R3, R3.2)
SG.AC-17	Access Control for Portable and Mobile Devices	AC-19	Access Control for Mobile Devices	2.15.25	Access Control for Portable and Mobile Devices	CIP 005-4a (R2, R2.1, R2.2, R2.4, R3, R3.2)
SG.AC-18	Use of External Information Control Systems	AC-20	Use of External Information Systems	2.15.29	Use of External Information Control Systems	CIP 005-4 (R2.4)
SG.AC-19	Control System Access Restrictions			2.15.28	External Access Protections	CIP 005-4a (R1.6) CIP 007-4 (R5)
SG.AC-20	Publicly Accessible Content	AC-22	Publicly Accessible Content			None
SG.AC-21	Passwords	IA-5	Authenticator Management	2.15.16	Passwords	CIP 007-4 (R5.3, R5.3.3)
Awareness and Training (SG.AT)						

- Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺
- Brian Mckay 11/13/12 9:55 PM
Deleted: May 2009
- Brian Mckay 11/13/12 9:58 PM
Deleted: CIP 005-2 (R2, R3, R3.1, R3.2)
- Victoria Pillitteri 1/3/13 11:21 AM
Formatted Table
- Brian Mckay 11/13/12 9:59 PM
Deleted: CIP 005-2 (R2.4, R5, R5.1)
- Victoria Pillitteri 1/3/13 11:21 AM
Formatted Table
- Victoria Pillitteri 1/3/13 11:20 AM
Deleted: SC-7
- Victoria Pillitteri 1/3/13 11:20 AM
Deleted: Boundary Protection
- Victoria Pillitteri 1/3/13 11:24 AM
Comment [20]: Changed to common tech from GRC
- Brian Mckay 11/13/12 10:00 PM
Deleted: CIP 007-2 (R5.3)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.AT-1	Awareness and Training Policy and Procedures	AT-1	Security Awareness and Training Policy and Procedures	2.11.1	Security Awareness Training Policy and Procedures	CIP 003-4 (R1, R2, R3) CIP 004-4 (R1, R2.1, R2.3) ▼
SG.AT-2	Security Awareness	AT-2	Security Awareness	2.11.2	Security Awareness	CIP 004-4 (R1) ▼
SG.AT-3	Security Training	AT-3	Security Training	2.11.3	Security Training	CIP 004-4 (R2, R2.1) ▼
SG.AT-4	Security Awareness and Training Records	AT-4	Security Training Records	2.11.4	Security Training Records	CIP 004-4 (R2.3) ▼
SG.AT-5	Contact with Security Groups and Associations	AT-5	Contact with Security Groups and Associations	2.11.5	Contact with Security Groups and Associations	None
SG.AT-6	Security Responsibility Training			2.11.6	Security Responsibility Training	CIP 004-4 (R2, R2.1, R2.2) ▼
SG.AT-7	Planning Process Training			2.7.5	Planning Process Training	CIP 004-4 (R2, R2.2) ▼
Audit and Accountability (SG.AU)						
SG.AU-1	Audit and Accountability	AU-1	Audit and Accountability Policy and Procedures	2.16.1	Audit and Accountability Process and Procedures	CIP 003-4 (R1, R2, R3, R5.3) CIP 007-4 (R5, R5.1.2, R5.2.3, R6.3-R6.5, R7.3, R9) ▼
SG.AU-2	Auditable Events	AU-2	Auditable Events	2.16.2	Auditable Events	CIP 005-4a (R3.2)

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:00 PM

Deleted: CIP 004-2 (R1, R2)

Brian Mckay 11/13/12 10:01 PM

Deleted: CIP 004-2 (R1)

Brian Mckay 11/13/12 10:01 PM

Deleted: CIP 004-2 (R2)

Brian Mckay 11/13/12 10:01 PM

Deleted: CIP 004-2 (R2.3)

Brian Mckay 11/13/12 10:02 PM

Deleted: CIP 004-2 (R2)

Brian Mckay 11/13/12 10:04 PM

Deleted: CIP 003-2 (R1, R1.1, R1.3)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
						CIP 006-4c (R7) CIP 007-4 (R5.1.2, R5.2.3, R6, R6.1, R6.3, R6.5) ▾ Enhancement: CIP 003-4 (R6) ▾
SG.AU-3	Content of Audit Records	AU-3	Content of Audit Records	2.16.3	Content of Audit Records	CIP 007-4 (R5.1.2, R6, R6.3) ▾
SG.AU-4	Audit Storage Capacity	AU-4	Audit Storage Capacity	2.16.4	Audit Storage	CIP 007-4 (R6.1) ▾
SG.AU-5	Response to Audit Processing Failures	AU-5	Response to Audit Processing Failures	2.16.5	Response to Audit Processing Failures	CIP 007-4 (R6.1) ▾
SG.AU-6	Audit Monitoring, Analysis, and Reporting	AU-6	Audit Monitoring, Analysis, and Reporting	2.16.6	Audit Monitoring, Process, and Reporting	CIP 004-4 (R3, R4.2, R4.2) CIP 005-4a (R3.2) CIP 007-4 (R5.1.2, R6.5) ▾
SG.AU-7	Audit Reduction and Report Generation	AU-7	Audit Reduction and Report Generation	2.16.7	Audit Reduction and Report Generation	CIP 007-4 (R5.1.2, R6.5) ▾
SG.AU-8	Time Stamps	AU-8	Time Stamps	2.16.8	Time Stamps	CIP 007-4 (R5.1.2, R6.3) ▾
SG.AU-9	Protection of Audit Information	AU-9	Protection of Audit Information	2.16.9	Protection of Audit Information	CIP 003-4 (R4, R4.1, R5) ▾

- Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺
- Brian Mckay 11/13/12 9:55 PM
Deleted: May 2009
- Victoria Pillitteri 1/3/13 11:28 AM
Deleted: AU-13
- Victoria Pillitteri 1/3/13 11:28 AM
Deleted: Monitoring for Information Disclosure
- Brian Mckay 11/13/12 10:05 PM
Deleted: CIP 005-2 (R1, R1.1, R1.3) - ... [5]
- Brian Mckay 11/13/12 10:05 PM
Formatted: Default
- Brian Mckay 11/13/12 10:05 PM
Formatted: Font:11.5 pt, English (US)
- Brian Mckay 11/13/12 10:05 PM
Deleted: CIP 007-3 (R5.1.2)
- Victoria Pillitteri 1/3/13 11:30 AM
Formatted Table
- Brian Mckay 11/13/12 10:06 PM
Formatted: Default
- Brian Mckay 11/13/12 10:06 PM
Formatted: Font:11.5 pt
- Victoria Pillitteri 1/3/13 11:30 AM
Comment [21]: Change to common tech from GRC
- Brian Mckay 11/13/12 10:06 PM
Deleted: CIP 007-2 (R5.1.2) - ... [6]
- Victoria Pillitteri 1/3/13 11:30 AM
Comment [22]: Change to common tech from GRC
- Victoria Pillitteri 1/3/13 11:30 AM
Comment [23]: Change to common tech from GRC
- Brian Mckay 11/13/12 10:07 PM
Deleted: CIP 003-2 (R4)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.AU-10	Audit Record Retention	AU-11	Audit Record Retention	2.16.10	Audit Record Retention	CIP 005-4a (R5.3) CIP 007-4 (R5.1.2, R6.4) CIP 008-4 (R2)
SG.AU-11	Conduct and Frequency of Audits	AU-1	Audit and Accountability Policy and Procedures	2.16.11	Conduct and Frequency of Audits	CIP 002-4 (R1) CIP 003-4 (R1.3, R4.3, R5.2) CIP 005-4a (R5.1)
SG.AU-12	Auditor Qualification			2.16.12	Auditor Qualification	None
SG.AU-13	Audit Tools			2.16.13	Audit Tools	CIP 007-4 (R6)
SG.AU-14	Security Policy Compliance	CA-1	Security Assessment and Authorization Policies and Procedures	2.16.14	Security Policy Compliance	CIP 003-4 (R1.3, R4.3, R5.2) CIP 005-4a (R5.1) CIP 008-4 (R1.4, R1.5, R1.6) CIP 009-4 (R2, R3, R5)
SG.AU-15	Audit Record Generation	AU-12	Audit Generation	2.16.15	Audit Generation	CIP 007-4 (R6)
SG.AU-16	Non-Repudiation	AU-10	Non-Repudiation	2.16.16	Non-Repudiation	CIP 003-4 (R6)
Security Assessment and Authorization (SG.CA)						

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:08 PM

Deleted: CIP 005-2 (R5.3) [7]

Victoria Pillitteri 1/3/13 11:31 AM

Deleted: AU-7

Victoria Pillitteri 1/3/13 11:31 AM

Deleted: Audit Reduction and Report Generation

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.CA-1	Security Assessment and Authorization Policy and Procedures	CA-1	Security Assessment and Authorization Policies and Procedures	2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures	CIP 003-4 (R3.3, R4.3) CIP 005-4a (R4.5) CIP 006-4 (R1.7, R8) CIP 007-4 (R1, R1.1, R2, R2.3, R3.2)
				2.17.1	Monitoring and Reviewing Control System Security management Policy and Procedures	
SG.CA-2	Security Assessments	CA-2	Security Assessments	2.17.3	Monitoring of Security Policy	CIP 003-4 (R3, R4.3) CIP 005-4a (R4) CIP 007-4 (R1, R1.1)
SG.CA-3	Continuous Improvement			2.17.2	Continuous Improvement	CIP 007-4 (R3, R3.2, R4, R4.2)
				2.17.4	Best Practices	
SG.CA-4	Information System Connections	CA-3	Information System Connection	2.18.5	Control System Connections	CIP 005-4a (R1.3, R1.6, R2, R2.5, R3, R3.1, R3.2, R4.3, R5.1) CIP 006-4c (R5) CIP 007-4 (R2)
SG.CA-5	Security Authorization to Operate	CA-6	Security Authorization	2.17.5	Security Accreditation	CIP 003-4 (R2, R2.2, R3.3)
		PM-10	Security Authorization Process			

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:10 PM

Deleted: CIP 005-2 (R2)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.CA-6	Continuous Monitoring	CA-7	Continuous Monitoring	2.18.7	Continuous Monitoring	CIP 003-4 (R3.3, R4.3) CIP 005-4a (R4.5) CIP 006-4 (R1.7, R8) CIP 007-4 (R1, R1.1, R2, R2.3, R3.2)
Configuration Management (SG.CM)						
SG.CM-1	Configuration Management Policy and Procedures	CM-1	Configuration Management Policy and Procedures	2.6.1	Configuration Management Policy and Procedures	CIP 003-4 (R1, R2, R3, R3.3, R4, R4.1, R4.2, R4.3, R6) CIP 005-4a (R2.2, R5, R5.1, R5.2) CIP 007-4 (R9) ▼
SG.CM-2	Baseline Configuration	CM-2	Baseline Configuration	2.6.2	Baseline Configuration	CIP 003-4 (R4) CIP 005-4a (R5.1) CIP 006-4c (R1.2) CIP 007-4 (R2, R9) ▼
SG.CM-3	Configuration Change Control	CM-3	Configuration Change Control	2.6.3	Configuration Change Control	CIP 003-4 (R6) CIP 005-4a (R5.1, R5.2)
		SA-10	Developer Configuration Management			CIP 007-4 (R1, R1.1, R1.2, R1.3, R3, R3.1, R3.2, R4.2, R9) ▼
SG.CM-4	Monitoring Configuration	CM-4	Security Impact Analysis	2.6.4	Monitoring Configuration	CIP 003-4 (R6)

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:11 PM

Deleted: CIP 003-2 (R6)

Brian Mckay 11/13/12 10:11 PM

Deleted: CIP 007-2 (R9)

Victoria Pillitteri 1/3/13 11:31 AM

Deleted: SA-10

Victoria Pillitteri 1/3/13 11:32 AM

Comment [24]: This cell needed to be split

Brian Mckay 11/13/12 10:11 PM

Deleted: CIP 003-2 (R6)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
	Changes	SA-10	Developer Configuration Management		Changes	CIP 007-4 (R1, R1.1, R1.2, R1.3, R3, R3.1) ▼
SG.CM-5	Access Restrictions for Configuration Change	CM-5	Access Restrictions for Change	2.6.5	Access Restrictions for Configuration Change	CIP 003-4 (R6) CIP 007-4 (R1, R5, R5.1, R5.1.2, R5.1.3, R5.2, R5.2.3) ▼
SG.CM-6	Configuration Settings	CM-6	Configuration Settings	2.6.6	Configuration Settings	CIP 003-4 (R2.4, R3, R3.1, R3.2, R3.3, R6) CIP 005-4a (R2.2) CIP 007-4 (R2.1 – R2.3, R3.2, R4.1, R9) ▼
SG.CM-7	Configuration for Least Functionality	CM-7	Least Functionality	2.6.7	Configuration for Least Functionality	CIP 005-4a (R2.2, R4.2) CIP 007-4 (R2, R2.1, R2.2, R8.2)
SG.CM-8	Component Inventory	CM-8	Information System Component Inventory	2.6.8	Configuration Assets	CIP 003-4 (R6) CIP 005-4a (R1, R1.2 – R1.4, R1.6, R2, R5.1, R5.2) CIP 006-4c (R1.1) CIP 007-4 (R3.2, R7.3, R9)
SG.CM-9	Addition, Removal, and Disposal of Equipment	MP-6	Media Sanitization	2.6.9	Addition, Removal, and Disposition of Equipment	CIP 003-4 (R6) CIP 007-4 (R7, R7.1, R7.2, R7.3) ▼

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:12 PM

Deleted: CIP 003-2 (R6)

Brian Mckay 11/13/12 10:12 PM

Deleted: CIP 003-2 (R6)

Brian Mckay 11/13/12 10:12 PM

Deleted: CIP 003-2 (R6) - [...](#) [8]

Brian Mckay 11/13/12 10:12 PM

Deleted: CIP 003-2 (R6)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.CM-10	Factory Default Settings Management			2.6.10	Factory Default Authentication Management	CIP 005-4a (R4.4) CIP 007-4 (R5.2.1, R8.3) ▼
SG.CM-11	Configuration Management Plan	CM-9	Configuration Management Plan			CIP 003-4 (R6)
Continuity of Operations (SG.CP)						
SG.CP-1	Continuity of Operations Policy and Procedures	CP-1	Contingency Planning Policy and Procedures			CIP 003-4 (R1, R2, R3) CIP 009-4 (R1, R4)
SG.CP-2	Continuity of Operations Plan	CP-1	Contingency Planning Policy and Procedures	2.12.2	Continuity of Operations Plan	CIP 008-4 (R1) CIP 009-4 (R1, R1.2, R4) ▼
SG.CP-3	Continuity of Operations Roles and Responsibilities	CP-2	Contingency Plan	2.12.3	Continuity of Operations Roles and Responsibilities	CIP 009-4 (R1.1, R1.2) ▼
SG.CP-4	Continuity of Operations Training					CIP 004-4 (R2.2.4)
SG.CP-5	Continuity of Operations Plan Testing	CP-4	Contingency Plan Testing and Exercises	2.12.5	Continuity of Operations Plan Testing	CIP 007-4 (R1.1, R1.2, R1.3, R9) CIP 008-4 (R1.6) CIP 009-4 (R2, R5) ▼ Enhancement: CIP 007-4 (R1.1)
SG.CP-6	Continuity of Operations Plan Update	CP-2	Contingency Plan	2.12.6	Continuity of Operations Plan Update	CIP 009-4 (R1, R3) ▼

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:13 PM

Deleted: CIP 005-2 (R4.4)

Brian Mckay 11/13/12 10:15 PM

Deleted: CIP 008-2 (R1) - ... [9]

Brian Mckay 11/13/12 10:15 PM

Deleted: CIP 009-2 (R1.1, R1.2) -

Brian Mckay 11/13/12 10:15 PM

Deleted: CIP 008-2 (R1.6) - ... [10]

Brian Mckay 11/13/12 10:15 PM

Deleted: CIP 009-2 (R4, R5)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.CP-7	Alternate Storage Sites	CP-6	Alternate Storage Sites	2.12.13	Alternative Storage Sites	CIP 009-4 (R4)
SG.CP-8	Alternate Telecommunication Services	CP-8	Telecommunications Services	2.12.14	Alternate Command/Control Methods	CIP 009-4 (R4)
SG.CP-9	Alternate Control Center	CP-7 CP-8	Alternate Processing Site Telecommunications Services	2.12.15	Alternate Control Center	CIP 009-4 (R4)
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	CP-10	Information System Recovery and Reconstitution	2.12.17	Control System Recovery and Reconstitution	CIP 003-4 (R4.1) CIP 005-4a (R4.4) CIP 007-4 (R8.3) CIP 009-4 (R4) Enhancement: CIP 005-4a (R4.4) CIP 007-4 (R8.3) CIP 009-4 (R4)
SG.CP-11	Fail-Safe Response			2.12.18	Fail-Safe Response	CIP 009-4 (R4)
Identification and Authentication (SG.IA)						
SG.IA-1	Identification and Authentication Policy and Procedures	IA-1	Identification and Authentication Policy and Procedures	2.15.2	Identification and Authentication Procedures and Policy	CIP 003-4 (R1, R2, R3) CIP 005-4a (R2.4, R2.5.1-R2.5.3) CIP 007-4 (R5, R9)
SG.IA-2	Identifier Management	IA-4	Identifier Management	2.15.4	Identifier Management	CIP 007-4 (R5.1.1)
SG.IA-3	Authenticator Management	IA-5	Authenticator Management	2.15.5	Authenticator Management	CIP 005-4a (R4.4) CIP 007-4 (R5, R5.1, R5.1.1, R5.3)

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:15 PM

Deleted: CIP 009-2 (R4)

Brian Mckay 11/13/12 10:17 PM

Deleted: CIP 007-2 (R5, R5.1, R5.2, R5.3)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.IA-4	User Identification and Authentication	IA-2	User Identification and Authentication	2.15.10	User Identification and Authentication	CIP 005-4a (R2.4) CIP 007-4 (R5) ↓
SG.IA-5	Device Identification and Authentication	IA-3	Device Identification and Authentication	2.15.12	Device Authentication and Identification	CIP 005-4a (R2) Enhancement: CIP 005-4a (R2.3, R2.4) ↓
SG.IA-6	Authenticator Feedback	IA-6	Authenticator Feedback	2.15.13	Authenticator Feedback	CIP 007-4 (R5) ↓
Information and Document Management (SG.ID)						
SG.ID-1	Information and Document Management Policy and Procedures			2.9.1	Information and Document Management Policy and Procedures	CIP 003-4 (R1,R2, R3, R4.1, R4.3, R5, R5.2, R5.3) CIP 005-4a (R1.6, R4.1, R5, R5.3) CIP 007-4 (R7, R9) CIP 008-4 (R2)
SG.ID-2	Information and Document Retention	SI-12	Information Output Handling and Retention	2.9.2	Information and Document Retention	CIP 005-4a (R1.6, R2.6, R5, R5.1 – R5.3) CIP 006-4c (R7) CIP 007-4 (R6.3 – R6.5, R7.3) ↓
SG.ID-3	Information Handling	MP-1	Media Protection Policy and Procedures	2.9.3	Information Handling	CIP 003-4 (R4.1) CIP 007-3 (R7, R7.3) ↓
SG.ID-4	Information Exchange			2.9.5	Information Exchange	None
SG.ID-5	Automated Labeling			2.9.11	Automated Labeling	None

Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM
Deleted: May 2009

Brian Mckay 11/13/12 10:17 PM
Deleted: CIP 003-2 (R1, R1.1, R1.3)

Brian Mckay 11/13/12 10:18 PM
Formatted: Default

Brian Mckay 11/13/12 10:18 PM
Formatted: Font:11.5 pt

Brian Mckay 11/13/12 10:18 PM
Formatted: Default

Brian Mckay 11/13/12 10:18 PM
Formatted: Font:11.5 pt

Brian Mckay 11/13/12 10:18 PM
Deleted: CIP 006-2 (R7)

Brian Mckay 11/13/12 10:18 PM
Deleted: CIP 003-2 (R4.1)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4	
Incident Response (SG.IR)							
SG.IR-1	Incident Response Policy and Procedures	IR-1	Incident Response Policy and Procedures	2.12.1	Incident Response Policy and Procedures	CIP 003-4 (R1, R2, R3) CIP 008-4 (R1, R1.1, R2)	
SG.IR-2	Incident Response Roles and Responsibilities	IR-1	Incident Response Policy and Procedures	2.7.4	Roles and Responsibilities	CIP 003-4 (R2, R2.3) CIP 008-4 (R1.2, R1.3) CIP 009-4 (R1.2)	
SG.IR-3	Incident Response Training	IR-2	Incident Response Training	2.12.4	Incident Response Training	CIP 004-4 (R2.2.4, R2.3)	
SG.IR-4	Incident Response Testing and Exercises	IR-3	Incident Response Testing and Exercises			CIP 007-4 (R1.1, R1.2, R1.3) CIP 008-4 (R1.6) CIP 009-4 (R2)	
SG.IR-5	Incident Handling	IR-4	Incident Handling	2.12.7	Incident Handling	CIP 009-4 (R1.1, R3)	
SG.IR-6	Incident Monitoring	IR-5	Incident Monitoring	2.12.8	Incident Monitoring	CIP 005-4a (R5.3) CIP 006-4c (R7) CIP 008-4 (R1.2, R2)	
SG.IR-7	Incident Reporting	IR-6	Incident Reporting	2.12.9	Incident Reporting	CIP 008-4 (R1.1, R1.3)	
SG.IR-8	Incident Response Investigation and Analysis	PE-6	Monitoring Physical Access	2.12.11	Incident Response Investigation and Analysis	CIP 008-4 (R1.4)	

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:19 PM

Deleted: CIP 008-2 (Rr1.2) .

... [11]

Brian Mckay 11/13/12 10:19 PM

Deleted: CIP 008-2 (R1, R1.2-R1.5) .

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.IR-9	Corrective Action	SI-11	Error Handling	2.12.12	Corrective Action	CIP 008-4 (R1.4) CIP 009-4 (R3)
SG.IR-10	Smart Grid Information System Backup	CP-9	Information System Backup	2.12.16	Control System Backup	CIP 009-4 (R4) Enhancement: CIP 009-4 (R4, R5)
SG.IR-11	Coordination of Emergency Response			2.2.4	Coordination of Threat Mitigation	CIP 004-4 (R2.1, R2.2.4) CIP 008-4 (R1.3)
Smart Grid Information System Development and Maintenance (SG.MA)						
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	MA-1	System Maintenance Policy and Procedures	2.10.1	System Maintenance Policy and Procedures	CIP 003-4 (R1, R2, R3) CIP 006-4c (R8) CIP 007-4 (R9)
SG.MA-2	Legacy Smart Grid Information System Updates			2.10.2	Legacy System Upgrades	CIP 003-4 (R6) CIP 007-4 (R1)
SG.MA-3	Smart Grid Information System Maintenance	PL-6	Security-Related Activity Planning	2.10.5	Unplanned System Maintenance	CIP 007-4 (R7, R7.2)
		MA-2	Controlled Maintenance	2.10.6	Periodic System Maintenance	CIP 009-4 (R4) Enhancement: CIP 007-4 (R7.3)
SG.MA-4	Maintenance Tools	MA-3	Maintenance Tools	2.10.7	Maintenance Tools	CIP 007-4 (R7)
SG.MA-5	Maintenance Personnel	MA-5	Maintenance Personnel	2.10.8	Maintenance Personnel	CIP 007-4 (R5, R5.2)

Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:19 PM

Deleted: CIP 008-2 (R1.4) [12]

Brian Mckay 11/13/12 10:20 PM

Deleted: CIP 008-2 (R1.3)

Victoria Pillitteri 1/3/13 11:34 AM
Comment [25]: This cell was originally 2 (weird formatting) and needed to be merged

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.MA-6	Remote Maintenance	MA-4	Non-Local Maintenance	2.10.9	Remote Maintenance	CIP 003-4 (R5) CIP 005-4a (R2, R2.3, R2.5.4, R3.1, R3.2) Enhancement: CIP 005-4a (R2.5.4) CIP 007-4 (R7)
SG.MA-7	Timely Maintenance	MA-6	Timely Maintenance	2.10.10	Timely Maintenance	CIP 009-4 (R4)
Media Protection (SG.MP)						
SG.MP-1	Media Protection Policy and Procedures	MP-1	Media Protection Policy and Procedures	2.13.1	Media Protection and Procedures	CIP 003-4 (R1, R2, R3, R4, R4.1, R4.3) CIP 004-4 (R2.2.3) CIP 007-4 (R9)
SG.MP-2	Media Sensitivity Level	RA-2	Security Categorization	2.13.3	Media Classification	CIP 003-4 (R4, R4.2)
				2.9.4	Information Classification	
SG.MP-3	Media Marking	MP-3	Media Marking	2.13.4	Media Labeling	CIP 003-4 (R4, R4.1)
				2.9.10	Automated Marking	
SG.MP-4	Media Storage	MP-4	Media Storage	2.13.5	Media Storage	CIP 006-4c (R1.1)
SG.MP-5	Media Transport	MP-5	Media Transport	2.13.6	Media Transport	CIP 003-4 (R5.1) CIP 007-4 (R7)
SG.MP-6	Media Sanitization and Disposal	MP-6	Media Sanitization	2.13.7	Media Sanitization and Storage	CIP 007-4 (R7, R7.1, R7.2, R7.3)
Physical and Environmental Security (SG.PE)						

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

Light Gray = Common Technical Requirement

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:22 PM

Deleted: CIP 009-2 (R4)

Brian Mckay 11/13/12 10:23 PM

Deleted: CIP 003-2 (R4, R4.2)

Victoria Pillitteri 1/3/13 11:34 AM

Deleted: et

Victoria Pillitteri 1/3/13 11:34 AM

Deleted: et

brian.mckay 11/14/12 4:33 PM

Formatted: Default

brian.mckay 11/14/12 4:33 PM

Formatted: Font:11.5 pt

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.PE-1	Physical and Environmental Security Policy and Procedures	PE-1	Physical and Environmental Protection Policy and Procedures	2.4.1	Physical and Environmental Security Policies and Procedures	CIP 003-4 (R1, R2, R3) CIP 005-4a (R1.6) CIP 006-4c (R1, R2, R7, R8) CIP 007-4 (R9) ▼
SG.PE-2	Physical Access Authorizations	PE-2	Physical Access Authorizations	2.4.2	Physical Access Authorizations	CIP 003-4 (R5.1) CIP 004-4 (R3, R4, R4.1) CIP 006-4c (R1.5) ▼
SG.PE-3	Physical Access	PE-3	Physical Access Control	2.4.3	Physical Access Control	CIP 004-4 (R4) CIP 006-4c (R2, R4, R3) CIP 007-4 (R5, R5.2.3) ▼ Enhancement: CIP 006-4c (R1.4, R4)
		PE-4	Access Control for Transmission Medium			
		PE-5	Access Control for Output Devices			
SG.PE-4	Monitoring Physical Access	PE-6	Monitoring Physical Access	2.4.4	Monitoring Physical Access	CIP 006-4c (R1.3, R4, R5, R6) CIP 008-4 (R1) ▼
SG.PE-5	Visitor Control	PE-7	Visitor Control	2.4.5	Visitor Control	CIP 006-4c (R1.4, R1.6) ▼
SG.PE-6	Visitor Records	PE-8	Access Records	2.4.6	Visitor Records	CIP 006-4c (R1.4, R1.6, R6) ▼
SG.PE-7	Physical Access Log Retention	PE-6	Monitoring Physical Access	2.4.7	Physical Access Log Retention	CIP 006-4c (R7) ▼

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:23 PM

Deleted: CIP 006-2 (R1, R2)

Brian Mckay 11/13/12 10:23 PM

Deleted: CIP 004-2 (R4)

Brian Mckay 11/13/12 10:23 PM

Deleted: CIP 006-2 (R2)

Brian Mckay 11/13/12 10:24 PM

Deleted: CIP 006-2 (R5)

Brian Mckay 11/13/12 10:24 PM

Deleted: CIP 006-2 (R1.4)

Brian Mckay 11/13/12 10:24 PM

Deleted: CIP 006-2 (R1.4, R6)

Victoria Pillitteri 1/3/13 11:35 AM

Formatted Table

Brian Mckay 11/13/12 10:24 PM

Deleted: CIP 006-2 (R7)

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement White = Common Governance, Risk and Compliance (GRC)						
Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.PE-8	Emergency Shutoff Protection	PE-10	Emergency Shutoff	2.4.8	Emergency Shutoff	None
SG.PE-9	Emergency Power	PE-11	Emergency Power	2.4.9	Emergency Power	None
SG.PE-10	Delivery and Removal	PE-16	Delivery and Removal	2.4.14	Delivery and Removal	CIP 003-4 (R6) CIP 007-4 (R7, R7.3) CIP 009-4 (R4)
SG.PE-11	Alternate Work Site	PE-17	Alternate Work Site	2.4.15	Alternate Work Site	None CIP 006-4c (R2)
SG.PE-12	Location of Smart Grid Information System Assets	PE-18	Location of Information System Components	2.4.18	Location of Control System Assets	CIP 006-4c (R2) CIP 006-4c (R7)
Planning (SG.PL)						
SG.PL-1	Strategic Planning Policy and Procedures	PL-1	Security Planning and Procedures	2.7.1	Strategic Planning Policy and Procedures	CIP 003-4 (R1, R2, R3)
SG.PL-2	Smart Grid Information System Security Plan	PL-2	System Security Plan	2.7.2	Control System Security Plan	CIP 003-4 (R4, R4.3)
SG.PL-3	Rules of Behavior	PL-4	Rules of Behavior	2.7.11	Rules of Behavior	CIP 004-4 (R1, R2)
SG.PL-4	Privacy Impact Assessment	PL-5	Privacy Impact Assessment			None
SG.PL-5	Security-Related Activity Planning	PL-6	Security-Related Activity Planning	2.7.12	Security-Related Activity Planning	CIP 007-4 (R1, R1.1)
Security Program Management (SG.PM)						
SG.PM-1	Security Policy and Procedures			2.1.1	Security Policies and Procedures	CIP 003-4 (R1, R2, R3, R5, R5.3)

- Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺
- Brian Mckay 11/13/12 9:55 PM
Deleted: May 2009
- Victoria Pillitteri 1/3/13 11:35 AM
Comment [26]: Changed to Common Tech from GRC
- Victoria Pillitteri 1/3/13 11:35 AM
Comment [27]: Changed to Common Tech from GRC
- Victoria Pillitteri 1/3/13 11:36 AM
Comment [28]: This entire row needs to be deleted.

- Brian Mckay 11/13/12 10:25 PM
Deleted: CIP 002-2 (R1)
- Victoria Pillitteri 1/3/13 1:00 PM
Deleted: AC-1
- Victoria Pillitteri 1/3/13 1:00 PM
Deleted: Access Control Policy and Procedures
- Brian Mckay 11/13/12 10:26 PM
Deleted: CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)
- Brian Mckay 11/13/12 10:26 PM
Formatted: Font:Bold

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.PM-2	Security Program Plan	PM-1	Information Security Program Plan			CIP 003-4 (R2, R2.2, R4.3)
SG.PM-3	Senior Management Authority	PM-2	Senior Information Security Officer			CIP 003-4 (R2)
SG.PM-4	Security Architecture	PM-7	Enterprise Architecture			None
SG.PM-5	Risk Management Strategy	PM-9	Risk Management Strategy			None
SG.PM-6	Security Authorization to Operate Process	PM-10	Security Authorization Process			None
SG.PM-7	Mission/Business Process Definition	PM-11	Mission/Business Process Definition			None
SG.PM-8	Management Accountability	PM-1	Information Security Program Plan	2.2.2	Management Accountability	CIP 003-4 (R2, R3, R5.2)
Personnel Security (SG.PS)						
SG.PS-1	Personnel Security Policy and Procedures	PS-1	Personnel Security Policy and Procedures	2.3.1	Personnel Security Policies and Procedures	CIP 003-4 (R1, R2, R3) CIP 004-3 R3 CIP 007-4 (R9)
SG.PS-2	Position Categorization	PS-2	Position Categorization	2.3.2	Position Categorization	CIP 004-4 (R3)
SG.PS-3	Personnel Screening	PS-3	Personnel Screening	2.3.3	Personnel Screening	CIP 004-4 (R3)
SG.PS-4	Personnel Termination	PS-4	Personnel Termination	2.3.4	Personnel Termination	CIP 004-4 (R4.1, R4.2) CIP 007-4 (R5, R5.2.3)

Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM
Deleted: May 2009

Brian Mckay 11/13/12 10:26 PM
Formatted: Font:Bold

Brian Mckay 11/13/12 10:26 PM
Formatted: Font:Bold

Brian Mckay 11/13/12 10:26 PM
Formatted: Font:Bold

Brian Mckay 11/13/12 10:26 PM
Deleted: CIP 003-2 (R2, R3)

Brian Mckay 11/13/12 10:27 PM
Deleted: CIP 004-2 (R3)

Brian Mckay 11/13/12 10:27 PM
Deleted: CIP 004-2 (R3)

Brian Mckay 11/13/12 10:27 PM
Deleted: CIP 004-2 (R3)

Brian Mckay 11/13/12 10:27 PM
Deleted: CIP 004-2 (R4.2)

... [13]

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.RA-3	Security Impact Level	RA-2	Security Categorization	2.18.8	Security Categorization	CIP 003-4 (R4, R4.1, R4.2, R4.3) CIP 003-4 (R4.3)
SG.RA-4	Risk Assessment	RA-3	Risk Assessment	2.18.9	Risk Assessment	CIP 003-4 (R6)
SG.RA-5	Risk Assessment Update	RA-3	Risk Assessment	2.18.10	Risk Assessment Update	CIP 003-4 (R3.3) CIP 005-4a (R4.5) CIP 007-4 (R1, R1.3, R2.3, R3.2, R8.4, R9)
SG.RA-6	Vulnerability Assessment and Awareness	RA-5	Vulnerability Scanning	2.18.11	Vulnerability Assessment and Awareness	CIP 003-4 (R6) CIP 005-4a (R4) CIP 007-4 (R2.3, R3.2, R8, R9) Enhancement: CIP 007-4 (R4, R4.2, R5)
Smart Grid Information System and Services Acquisition (SG.SA)						
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	SA-1	System and Services Acquisition Policy and Procedures	2.5.1	System and Services Acquisition Policy and Procedures	CIP 003-4 (R1, R2, R3) CIP 007-4 (R9)
SG.SA-2	Security Policies for Contractors and Third Parties	PS-7	Third-Party Personnel Security	2.2.5	Security Policies for Third Parties	CIP 004-4 (R2.1, R3, R4.1, R4.2) CIP 007-4 (R5, R5.2.3)
				2.2.6	Termination of Third-Party Access	
SG.SA-3	Life-Cycle Support	SA-3	Life-Cycle Support	2.5.3	Life-Cycle Support	None

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:29 PM

Deleted: CIP 002-2 (R1.2)

Brian Mckay 11/13/12 10:29 PM

Deleted: CIP 002-2 (R4)

Brian Mckay 11/13/12 10:29 PM

Deleted: CIP 005-2 (R4, R4.2, R4.3, R4.4, R4.5, R4.6, R4.7, R4.8, R4.9, R4.10, R4.11, R4.12, R4.13, R4.14, R4.15)

Brian Mckay 11/13/12 10:29 PM

Formatted: Default

Brian Mckay 11/13/12 10:29 PM

Formatted: Font:11.5 pt, English (US)

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement White = Common Governance, Risk and Compliance (GRC)						
Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.SA-4	Acquisitions	SA-4	Acquisitions	2.5.4	Acquisitions	None
SG.SA-5	Smart Grid Information System Documentation	SA-5	Information System Documentation	2.5.5	Control System Documentation	None
SG.SA-6	Software License Usage Restrictions	SA-6	Software Usage Restrictions	2.5.6	Software License Usage Restrictions	None
SG.SA-7	User-Installed Software	SA-7	User-Installed Software	2.5.7	User-installed Software	CIP 007-4 (R3, R5)
SG.SA-8	Security Engineering Principles	SA-8 SA-13	Security Engineering Principles Trustworthiness	2.5.8	Security Engineering Principals	CIP 007-4 (R1, R1.1, R1.2, R1.3)
SG.SA-9	Developer Configuration Management	SA-10	Developer Configuration Management	2.5.10	Vendor Configuration Management	CIP 003-4 (R6)
SG.SA-10	Developer Security Testing	SA-11	Developer Security Testing	2.5.11	Vendor Security Testing	CIP 007-4 (R1, R1.1 – R1.3)
SG.SA-11	Supply Chain Protection	SA-12	Supply Chain Protection	2.5.12	Vendor Life-cycle Practices	CIP 007-4 (R1, R1.3, R3, R4, R4.2)
Smart Grid Information System and Communication Protection (SG.SC)						
SG.SC-1	System and Communication Protection Policy and Procedures	SC-1	System and Communication Protection Policy and Procedures	2.8.1	System and Communication Protection Policy and Procedures	CIP 003-4 (R1, R2, R3) CIP 005-4 (R1.1 - R1.3) CIP 007-4 (R9)
SG.SC-2	Communications Partitioning			2.8.2	Management Port Partitioning	None
SG.SC-3	Security Function Isolation	SC-3	Security Function Isolation	2.8.3	Security Function Isolation	None
SG.SC-4	Information Remnants	SC-4	Information in Shared Resources	2.8.4	Information Remnants	CIP 007-4 (R7, R7.1, R7.2)

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Victoria Pillitteri 1/3/13 1:01 PM

Formatted Table

Victoria Pillitteri 1/3/13 1:01 PM

Comment [29]: Changed to GRC from Common Tech

Victoria Pillitteri 1/3/13 1:01 PM

Comment [30]: Changed to GRC from Common Tech

Brian Mckay 11/13/12 10:30 PM

Deleted: CIP 003-2 (R1, R1.1, R1.3)

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.SC-5	Denial-of-Service Protection	SC-5	Denial-of-Service Protection	2.8.5	Denial-of-Service Protection	None
SG.SC-6	Resource Priority	SC-6	Resource Priority	2.8.6	Resource Priority	None
SG.SC-7	Boundary Protection	SC-7	Boundary Protection	2.8.7	Boundary Protection	CIP 005-4a (R1, R1.2, R1.3, R1.6, R2, R2.2, R2.3, R2.4, R3, R3.1, R3.2) CIP 007-4 (R2.1), Enhancement: CIP 005-4a (R2.1, R2.4)
SG.SC-8	Communication Integrity	SC-8	Transmission Integrity	2.8.8	Communication Integrity	None
SG.SC-9	Communication Confidentiality	SC-9	Transmission Confidentiality	2.8.9	Communication Confidentially	None
SG.SC-10	Trusted Path	SC-11	Trusted Path	2.8.10	Trusted Path	None
SG.SC-11	Cryptographic Key Establishment and Management	SC-12	Cryptographic Key Establishment and Management	2.8.11	Cryptographic Key Establishment and Management	None
SG.SC-12	Use of Validated Cryptography	SC-13	Use of Cryptography	2.8.12	Use of Validated Cryptography	None
SG.SC-13	Collaborative Computing	SC-15	Collaborative Computing Devices	2.8.13	Collaborative Computing	None
SG.SC-14	Transmission of Security Parameters	SC-16	Transmission of Security Attributes	2.8.14	Transmission of Security Parameters	None
SG.SC-15	Public Key Infrastructure Certificates	SC-17	Public Key Infrastructure Certificates	2.8.15	Public Key Infrastructure Certificates	None
SG.SC-16	Mobile Code	SC-18	Mobile Code	2.8.16	Mobile Code	CIP 007-4 (R4)

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

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Brian Mckay 11/13/12 10:31 PM

Deleted: CIP 005-2 (R1, R1.1, R1.2, R1.3, R1.4, R1.6, R2, R2.1-R2.4, R5, R5.1)

Brian Mckay 11/13/12 10:32 PM

Formatted: Default

Brian Mckay 11/13/12 10:32 PM

Formatted: Font:11.5 pt

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.SC-17	Voice-Over Internet Protocol	SC-19	Voice Over Internet Protocol	2.8.17	Voice-over-Internet Protocol	None
SG.SC-18	System Connections	CA-3	Information System Connections	2.8.18	System Connections	CIP 005-4a (R1, R1.3, R1.5, R2, R2.2-R2.4, R3, R3.1, R3.2) CIP 006-4c (R1)
SG.SC-19	Security Roles			2.8.19	Security Roles	CIP 003-4 (R5.2)
SG.SC-20	Message Authenticity			2.8.20	Message Authenticity	None
SG.SC-21	Secure Name/Address Resolution Service	SC-20	Secure Name/Address Resolution Service (Authoritative Source)	2.8.22	Secure Name/Address Resolution Service (Authoritative Source)	None
SG.SC-22	Fail in Known State	SC-24	Fail in Known State	2.8.24	Fail in Know State	None
SG.SC-23	Thin Nodes	SC-25	Thin Nodes	2.8.25	Thin Nodes	None
SG.SC-24	Honeypots	SC-26	Honeypots	2.8.26	Honeypots	None
SG.SC-25	Operating System-Independent Applications	SC-27	Operating System-Independent Applications	2.8.27	Operating System-Independent Applications	None
SG.SC-26	Confidentiality of Information at Rest	SC-28	Confidentiality of Information at Rest	2.8.28	Confidentiality of Information at Rest	None
SG.SC-27	Heterogeneity	SC-29	Heterogeneity	2.8.29	Heterogeneity	None
SG.SC-28	Virtualization Technique	SC-30	Virtualization Technique	2.8.30	Virtualization Techniques	None
SG.SC-29	Application Partitioning	SC-2	Application Partitioning	2.8.32	Application Partitioning	CIP 007-4 (R5.2)
SG.SC-30	Information System Partitioning	SC-32	Information Systems Partitioning			None
Smart Grid Information System and Information Integrity (SG.SI)						

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

Light Gray = Common Technical Requirement

Victoria Pillitteri 1/3/13 11:29 AM

Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM

Deleted: May 2009

Victoria Pillitteri 1/3/13 1:01 PM

Formatted Table

Brian Mckay 11/13/12 10:32 PM

Deleted: CIP 005-2 (R2, R2.2-R2.4)

Victoria Pillitteri 1/3/13 1:02 PM

Comment [31]: Changed to GRC from Common Tech

Victoria Pillitteri 1/3/13 1:02 PM

Deleted: SA-9

Victoria Pillitteri 1/3/13 1:02 PM

Deleted: External Information System Services

Brian Mckay 11/13/12 10:32 PM

Deleted: CIP 003-2 (R5)

Victoria Pillitteri 1/3/13 1:02 PM

Deleted: SC-8

Victoria Pillitteri 1/3/13 1:02 PM

Deleted: Transmission Integrity

Brian Mckay 11/13/12 10:32 PM

Formatted: Default

Brian Mckay 11/13/12 10:32 PM

Formatted: Font:11.5 pt

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.SI-1	System and Information Integrity Policy and Procedures	SI-1	System and Information Integrity Policy and Procedures	2.14.1	System and Information Integrity Policy and Procedures	CIP 003-4 (R1, R2, R3)
SG.SI-2	Flaw Remediation	SI-2	Flaw Remediation	2.14.2	Flaw Remediation	CIP 003-4 (R6) CIP 005-4a (R4) CIP 007-4 (R3, R3.1, R3.2, R8) ▾
SG.SI-3	Malicious Code and Spam Protection	SI-3	Malicious Code Protection	2.14.3	Malicious Code Protection	CIP 007-4 (R4, R4.1, R4.2) ▾
		SI-8	Spam Protection	2.14.8	Spam Protection	CIP 005-4a (R1.5, R3, R3.1, R3.2) CIP 007-4 (R4, R6, R6.1 – R6.5) ▾
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	SI-4	Information System Monitoring	2.14.4	System Monitoring Tools and Techniques	CIP 003-4 (R6) CIP 004-4 (R1) ▾
SG.SI-5	Security Alerts and Advisories	SI-5	Security Alerts, Advisories, and Directives	2.14.5	Security Alerts and Advisories	CIP 003-4 (R1, R2, R3)
SG.SI-6	Security Functionality Verification	SI-6	Security Functionality Verification	2.14.6	Security Functionality Verification	CIP 003-4 (R4.3) CIP 005-4a (R3.2, R4) CIP 007-4 (R1) ▾
SG.SI-7	Software and Information Integrity	SI-7	Software and Information Integrity	2.14.7	Software and Information Integrity	None
SG.SI-8	Information Input Validation	SI-10	Information Input Validation	2.14.9	Information Input Restrictions	CIP 003-4 (R5) ▾

- Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺
- Brian Mckay 11/13/12 9:55 PM
Deleted: May 2009
- Victoria Pillitteri 1/3/13 1:03 PM
Formatted Table
- Brian Mckay 11/13/12 10:33 PM
Deleted: CIP 007-2 (R3, R3.1, R3.2)
- Victoria Pillitteri 1/3/13 1:03 PM
Comment [32]: Change to Common Tech from GRC
- Brian Mckay 11/13/12 10:33 PM
Deleted: CIP 007-2 (R4, R4.1, R4.2)
- Brian Mckay 11/13/12 10:33 PM
Deleted: CIP 007-2 (R4)
- Victoria Pillitteri 1/3/13 1:03 PM
Comment [33]: Change to Common Tech from GRC
- Brian Mckay 11/13/12 10:33 PM
Deleted: CIP 007-2 (R6)
- Brian Mckay 11/13/12 10:33 PM
Deleted: CIP 007-2 (R1)
- Brian Mckay 11/13/12 10:33 PM
Deleted: CIP 003-2 (R5) [16]

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 4
SG.SI-9	Error Handling	SI-11	Error Handling	2.14.11	Error Handling	None

Victoria Pillitteri 1/3/13 11:29 AM
Comment [19]: Tanya – can you please make all of the font in this column formatted to the same style/size as the rest of the table? Thank you! ☺

Brian Mckay 11/13/12 9:55 PM
 Deleted: May 2009

DRAFT