



SMART GRID INTEROPERABILITY PANEL

1  
2  
3  
4  
5  
6

7 **Guide for Assessing the High-Level**  
8 **Security Requirements in NISTIR 7628,**  
9 **Guidelines for Smart Grid Cyber**  
10 **Security**

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29

30 **SGIP Document Number: CSWG-TC-001, Version 0.9**  
31 **Document Source: December 20, 2011**  
32 **Author/Editor: SGIP CSWG - Test & Certification Subgroup**  
33 **Production Date: December 20, 2011**  
34

35 **RIGHT TO DISTRIBUTE AND CREDIT NOTICE**

36  
37 This material was created by the Smart Grid Interoperability Panel Cybersecurity  
38 Working Group Testing and Certification Subgroup and is available for public use  
39 and distribution. Please include credit in the following manner: Guide for Assessing  
40 the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid  
41 Cyber Security, CSWG-TC-001. © December 20, 2011. *All rights reserved by the*  
42 *SGIP.*

43  
44 **DISCLAIMER**

45  
46  
47 *This document is a work product of the SGIP. It was prepared by the participants of*  
48 *the SGIP and approved by the Smart Grid Interoperability Panel's Plenary Leadership.*  
49 *Neither the National Institute of Standards and Technology (NIST), the SGIP*  
50 *leadership, its members nor any person acting on behalf of any of the above:*

- 51
- 52 • *MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, with*  
53 *respect to the accuracy, completeness, or usefulness of the information*  
54 *contained in this report, or that the use of any information, apparatus, process,*  
55 *or composition disclosed in this report may not infringe privately owned rights;*  
56 *or*
  - 57 • *Assumes any liabilities with respect to the use of, or for damages resulting from*  
58 *the use of, any information, apparatus, process, or composition disclosed in this*  
59 *report.*
  - 60 • *Reference herein to any specific commercial product, process, or service by*  
61 *trade name, trademark, manufacturer, or otherwise, does not necessarily*  
62 *constitute or imply its endorsement, recommendation, or favoring by the Smart*  
63 *Grid Interoperability Panel.*

64  
65 **THIS IS NOT A NIST DOCUMENT**

## THE SGIP

66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79

The Smart Grid Interoperability Panel (SGIP) is a membership-based organization created by an Administrator under a contract from NIST to provide an open process for stakeholders to participate in providing input and cooperating with NIST in the ongoing coordination, acceleration and harmonization of standards development for the Smart Grid. The SGIP also reviews use cases, identifies requirements and architectural reference models, coordinates and accelerates Smart Grid testing and certification, and proposes action plans for achieving these goals. The SGIP does not write standards, but serves as a forum to coordinate the development of standards and specifications by many standards setting organizations.

DRAFT

80 **Contents**

81 1. Introduction..... 5  
82 1.1 Purpose..... 6  
83 1.2 NISTIR 7628 Background..... 6  
84 1.3 Target Audience..... 7  
85 2. Fundamentals ..... 9  
86 2.1 High-Level Security Requirements..... 9  
87 2.2 Security Assessment Objectives..... 11  
88 2.3 Assessment Methods..... 12  
89 3. Security Assessment Process..... 15  
90 3.1 Preparing for Security Requirement Assessments..... 15  
91 3.2 Developing Security Assessment Plans..... 16  
92 3.2.1 Determine which security requirements are to be assessed..... 17  
93 3.2.2 Select appropriate procedures to assess the security requirements ..... 17  
94 3.2.3 Tailor assessment procedures for specific operating environments ..... 17  
95 3.2.4 Optimize selected assessment procedures to ensure maximum efficiency..... 18  
96 3.2.5 Finalize security assessment plan and obtain approval to execute plan ..... 18  
97 3.3 Conducting Security Requirement Assessments..... 18  
98 3.4 Analyzing Security Assessment Report Results ..... 19  
99 4. Revision History..... 21  
100 5. Contributors ..... 21  
101 Appendix A – NIST SP800-53A Assessment Method Definitions..... 22  
102 Appendix B – Assessment Procedures Catalog..... 23

103 **Tables**

104 Table 1. Sample NISTIR 7628 high-level security requirement, SG.MP-3, Media Marking... 11  
105 Table 2. SG.MP-3, Media Marking Assessment Objective ..... 12  
106 Table 3. SG.MP-3, Media Marking Assessment Method..... 13

107 **Figures**

108 Figure 1. Smart Grid Security Requirement Assessment Process Overview ..... 20  
109  
110

111 **1. Introduction**

112 The United States has embarked on a major transformation of its electric power  
113 infrastructure. This vast infrastructure upgrade—extending from homes and businesses to  
114 power generating plants and wind farms, affecting nearly everyone and everything in  
115 between—is central to national efforts to increase energy efficiency, reliability, and  
116 security; transitioning to renewable sources of energy; reduction of greenhouse gas  
117 emissions; and building a sustainable economy that ensures future prosperity. These and  
118 other prospective benefits of “smart” electric power grids are being pursued not only in the  
119 United States, but worldwide.

120  
121 Steps to transform the nation’s aging electric power grid into an advanced, digital  
122 infrastructure with two-way capabilities for communicating information, controlling  
123 equipment, and distributing energy will take place over many years. In concert with these  
124 developments and the underpinning public and private investments, key enabling activities  
125 also must be accomplished. Chief among them is devising effective strategies for protecting  
126 the privacy of Smart Grid-related data and for securing the computing and communication  
127 networks that will be central to the performance and availability of the envisioned electric  
128 power infrastructure. While integrating information technologies is essential to building  
129 the Smart Grid and realizing its benefits, networked technologies add complexity and also  
130 introduce new interdependencies and vulnerabilities. Approaches to secure the  
131 information and communication technologies and to protect privacy must be designed and  
132 implemented early in the transition to the Smart Grid.

133  
134 As the transition to the Smart Grid occurs, the electricity sector becomes increasingly  
135 dependent on information technology (IT)<sup>1</sup> (i.e., hardware, software, and firmware),  
136 processes, industrial control systems (ICS)<sup>2</sup> and people, working together to provide  
137 organizations with the capability to process, store, and transmit information and  
138 commands in a timely manner to support various missions and business functions. The  
139 degree to which organizations depends upon IT systems and ICS<sup>3</sup> to conduct routine,  
140 important, and critical mission and business functions means that the protection of the  
141 underlying systems is paramount to the success of the organization. The selection of  
142 appropriate security requirements for Smart Grid information systems is an important task  
143 that can have major implications on the operations and assets of an organization. Security  
144 requirements are the management, operational, and technical safeguards or  
145 countermeasures prescribed for Smart Grid information systems to protect the  
146 confidentiality, integrity (including non-repudiation and authenticity), and availability of  
147 the system and its information. Once employed, security requirements are assessed to

---

<sup>1</sup> IT is a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate (i.e., people, processes, technologies, and facilities).

<sup>2</sup> ICS is a set of hardware and software acting in concert that manages the behavior of other devices in the electrical grid.

<sup>3</sup> For this document, the term Smart Grid information system implies IT systems and / or ICS.

148 gather the information necessary to determine overall effectiveness of the requirements;  
149 that is, the extent to which the requirements are implemented correctly, operating as  
150 intended, and producing the desired security posture for the Smart Grid information  
151 system. Understanding the overall effectiveness of the security requirements implemented  
152 in the Smart Grid information system and its operational environment is essential in  
153 determining the risk to the organization's operations.

154  
155 The NIST Interagency Report (IR) 7628, *Guidelines for Smart Grid Cyber Security*, published  
156 in August 2010, documents high-level security requirements in volume one. This SGIP  
157 document, *Guide for Assessing the High-Level Security Requirements in the NISTIR 7628*  
158 provides:

- 159
- 160 • Guidance on how to develop an assessment program to determine compliance with
- 161 the NISTIR 7628 high level security requirements ; and
- 162 • A baseline set of assessment objectives and procedures for conducting a security
- 163 assessment.<sup>4</sup>

## 164 **1.1 Purpose**

165 Security assessments are not about checklists, simple pass-fail results, or generating  
166 paperwork to pass inspections or audits—rather, they are the principal vehicle used to  
167 verify that the implementers and operators of Smart Grid information systems including  
168 the telecommunications infrastructures are meeting their stated security goals and  
169 objectives. This guide is written to provide a foundation to facilitate a security assessment  
170 based on the NISTIR 7628 high-level security requirements implemented within an  
171 effective risk management program. The security assessment results provide senior  
172 executives:

- 173
- 174 • Evidence about the effectiveness of security requirements in Smart Grid information
- 175 systems and their environments;
- 176 • An indication of the quality of the risk management processes employed within the
- 177 organization; and
- 178 • Information about the strengths and weaknesses of Smart Grid information systems
- 179 which are supporting critical missions and applications in a global environment of
- 180 sophisticated threats.

181  
182 A well-executed security assessment provides realistic information about the validity of the  
183 organization's implementation of their security plan.

## 184 **1.2 NISTIR 7628 Background**

185 The three-volume report, *Guidelines for Smart Grid Cyber Security* (NISTIR 7628), presents  
186 an analytical framework that organizations can use to develop effective cybersecurity

---

<sup>4</sup> Appendix B provides an assessment procedure catalog that allows an organization to customize requirements, assessment objectives, assessment methods, and assessment objects for an organization Smart Grid information system specific assessment.

187 strategies tailored to their particular combinations of Smart Grid-related characteristics,  
188 risks, and vulnerabilities. The electricity sector is a diverse community of stakeholders—  
189 from utilities to providers of energy management services, to manufacturers of electric  
190 vehicles and charging stations. Any electricity sector enterprise can adopt, partially or in  
191 full, the methods and supporting information presented in the NISTIR 7628 as normative  
192 requirements for assessing their cybersecurity risk, and identifying and applying  
193 appropriate security requirements. This approach recognizes that the electric grid is  
194 changing from a relatively isolated system to a complex, highly interconnected  
195 environment. As the electric grid continues to evolve, each organization’s cybersecurity  
196 requirements should progress as technology advances and threats to grid security multiply  
197 and diversify.

198  
199 The three volumes that make up the NISTIR 7628 are intended primarily for individuals  
200 and organizations responsible for addressing Smart Grid information system cybersecurity.  
201 As a result of the pervasiveness of the electric power infrastructure and its growing  
202 importance in the U.S. economy, these individuals and organizations comprise a large and  
203 diverse group that includes vendors of energy information and management services,  
204 equipment manufacturers, utilities, system operators, regulators, researchers, and network  
205 specialists. In addition, the NISTIR 7628 incorporates the perspectives of three primary  
206 industries converging on opportunities enabled by the emerging Smart Grid—utilities and  
207 other businesses in the electricity sector, the information technology industry, and the  
208 telecommunications sector. The NISTIR 7628 describes the approach, including the risk  
209 assessment process, used by the SGIP Cybersecurity Working Group (CSWG) to identify  
210 high-level security requirements. It also presents a high-level architecture followed by a  
211 sample logical interface reference model used to identify and define logical interface  
212 categories and across the seven Smart Grid domains. High-level security requirements for  
213 each of the logical interface categories are then described.

### 214 **1.3 Target Audience**

215 This guide is for any utility, testing laboratory, regulator, auditor, or security group to assist  
216 in the development of a cybersecurity assessment program and to assess the organization’s  
217 Smart Grid information systems and environment against the NISTIR 7628 high-level  
218 security requirements.

219  
220 This guide intends to serve a diverse group of Smart Grid information system and  
221 information security professionals, including individuals responsible for:

- 222  
223 • Information system and security requirement assessment and monitoring (e.g.,  
224 system evaluators, assessors/assessment teams, certification agents/certification  
225 teams, independent verification and validation assessors, auditors, , information  
226 system owners);
- 227 • Information system and security management and oversight (e.g., senior  
228 information security officers, information security managers);
- 229 • Information security implementation and operation (e.g., information system  
230 owners, mission / business owners, and information system security officers); and

- 231
- 232
- 233
- 234
- Information system development and integration (e.g., program managers, information technology product developers, information system developers, systems integrators).

DRAFT

235 **2. Fundamentals**

236 This Chapter describes the three basic concepts needed when assessing the high-level  
 237 security requirements in Smart Grid information systems: 1) identifying the high-level  
 238 security requirements; 2) security assessment objectives; and 3) assessment methods and  
 239 the corresponding assessment objects.

240 **2.1 High-Level Security Requirements**

241 The organization's security plan provides an overview of the security requirements for the  
 242 Smart Grid information systems and describes the procedural and technical mechanisms to  
 243 be implemented to satisfy those requirements.

244  
 245 The NISTIR 7628 describes high-level security requirements that are applicable to the  
 246 entire Smart Grid or to particular domains, such as generation or distribution, and interface  
 247 categories. Power system operations pose many security challenges that are different from  
 248 the challenges faced by most other industries and within power system operational  
 249 environments. In particular, there are strict performance and reliability requirements that  
 250 power system operations need to meet. The requirements in the NISTIR 7628 that help  
 251 ensure performance and reliability needs were selected from a larger collection of  
 252 requirements reviewed by the CSWG.<sup>5</sup>

253  
 254 Each of the high-level security requirements is assigned to one of the three categories  
 255 where a particular requirement is most applicable within an organization, operation, or  
 256 function. The categories are:

- 257
- 258 • **Governance, risk, and compliance (GRC) requirements:** Addresses requirements
- 259 at the Smart Grid organizational level;
- 260 • **Common technical requirements:** Applicable to all interfaces; and
- 261 • **Unique technical requirements:** Applicable to zero or more—but not all—
- 262 interfaces. Some of these requirements are not assigned to an interface category,
- 263 but exist for the readers' consideration.
- 264

265 The common and unique technical requirements should be allocated to each Smart Grid  
 266 information system, but not necessarily to every component<sup>6</sup> within a system, as the focus  
 267 is on system level security and not on specific information exchanges between components.  
 268 Each organization should develop a security architecture for each Smart Grid information

---

<sup>5</sup> Sources include NIST SP 800-53, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, *Building Effective Security Assessment Plans*, Department of Homeland Security Catalog of Control Systems Security: Recommendations for Standards Developers, NERC Critical Infrastructure Protection Standards (CIPS), and Nuclear Regulatory Commission Regulatory Guidance.

<sup>6</sup> Components include for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors, field bus, and control network), operating systems, middleware, applications, programmable logic controller hardware, remote terminal unit, actuators, diagnostics, and intelligent electronic devices.

269 system and allocate appropriate security requirements. Some security requirements may  
270 be allocated to one or more Smart Grid information systems. Impact levels<sup>7</sup> for a specific  
271 Smart Grid information system—and, therefore, the need to implement requirement  
272 enhancements to specific requirements— will be determined by organizations during the  
273 risk assessment process.

274  
275 In addition, organizations may find it necessary to identify compensating security  
276 requirements. A compensating security requirement is implemented by an organization in  
277 lieu of a recommended security requirement to provide equivalent or comparable level of  
278 protection for the Smart Grid information system and the information processed, stored, or  
279 transmitted by that Smart Grid information system. More than one compensating  
280 requirement may be necessary to provide the equivalent or comparable protection for a  
281 particular security requirement. For example, an organization with significant staff  
282 limitations may compensate for the recommended separation of duty security requirement  
283 by strengthening the audit, accountability, and personnel security requirements within the  
284 Smart Grid information system.

285  
286 Each NISTIR 7628 high-level security requirement is presented in a standard format with  
287 the following information:

- 288
- 289 • *Security requirement identifier and name.* Each security requirement has a  
290 unique identifier that consists of three components. The initial component is SG  
291 – for Smart Grid. The second component is the family name, e.g., AC for Access  
292 Control and CP for Continuity of Operations. The third component is a unique  
293 numeric identifier, for example, SG.AC-1 and SG.CP-3. Each requirement also has  
294 a unique descriptive name.
  - 295 • *Category.* This identifies whether the security requirement is a GRC, common  
296 technical or unique technical requirement. For each common technical security  
297 requirement, the most applicable objective (confidentiality, integrity, and  
298 availability) is listed.
  - 299 • The *Requirement* describes specific security-related activities or actions to be  
300 carried out by the organization or by the Smart Grid information system.
  - 301 • The *Supplemental Guidance* section provides additional information that may be  
302 useful in understanding the security requirement.
  - 303 • The *Requirement Enhancements* section provides additional capability to (i)  
304 build additional functionality to a requirement, and / or (ii) increase the  
305 strength of a requirement. In both cases, the requirement enhancements are to  
306 be considered in Smart Grid information systems requiring greater protection  
307 due to the potential impact of hardware or data loss based on the results of a risk  
308 assessment. Requirement enhancements are numbered sequentially within each  
309 requirement.

---

<sup>7</sup>The three impact levels, i.e., low, moderate, and high is based upon the expected adverse effect of a security breach upon organizational operations, assets, or individuals. NISTIR 7628, Section 3.3 Impact Levels for the confidentiality, integrity, and availability (CI&A) categories provides additional information.

- 310 • The *Additional Considerations* provide additional statements of security
- 311 capability that may be used to enhance the associated security requirement.
- 312 These are provided for organizations to consider as they implement Smart Grid
- 313 information systems and are not intended as security requirements. Each
- 314 additional consideration is numbered A1, A2, etc., to distinguish them from the
- 315 security requirements and requirement enhancements.
- 316 • The *Impact Level Allocation* identifies the security requirement and associated
- 317 enhancements, as applicable, at each impact level: low, moderate, and high. The
- 318 impact levels for a specific Smart Grid information system will be determined by
- 319 the organization in the risk assessment process.

320 **Table 1. Sample NISTIR 7628 high-level security requirement, SG.MP-3, Media Marking**

<b>SG.MP-3 Media Marking</b>		
<b>Category:</b> Common Governance, Risk, and Compliance (GRC) Requirements		
<b>Requirement</b> The organization marks removable Smart Grid information system media and Smart Grid information system output in accordance with organization-defined policy and procedures.		
<b>Supplemental Guidance</b> 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).		
<b>Requirement Enhancements</b> None.		
<b>Additional Considerations</b> None.		
<b>Impact Level Allocation</b>		
Low: Not Selected	Moderate: SG. MP-3	High: SG. MP-3

322

## 323 **2.2 Security Assessment Objectives**

324 An assessment procedure consists of a set of assessment objectives, each with an

325 associated set of potential assessment methods and objects. An assessment objective

326 includes a set of determination statements related to the particular security requirement<sup>8</sup>

327 being assessed. The determination statements are closely linked to the content of the

328 NISTIR 7628 high-level security requirements to ensure traceability of assessment results

329 back to a fundamental requirement. The application or execution of an assessment

330 procedure to a security requirement produces assessment findings. These assessment

331 findings provide realistic information about the validity of the organization's

332 implementation of their security plan.

333

334 The assessment objectives identify the following items to be assessed:

335

---

<sup>8</sup> Security requirements under assessment also include any requirement enhancements.

- 336 • **Specifications** are the document-based artifacts (e.g., policies, procedures, plans,  
337 system security requirements, functional specifications, and architectural designs)  
338 associated with a Smart Grid information system.
- 339 • **Mechanisms** are the specific hardware, software, or firmware safeguards and  
340 countermeasures employed within a Smart Grid information system.<sup>9</sup>
- 341 • **Activities** are the specific protection-related pursuits or actions supporting a Smart  
342 Grid information system that involve people (e.g., conducting system backup  
343 operations, monitoring network traffic, exercising a contingency plan).
- 344 • **Individuals**, or groups of individuals, are people applying the specifications,  
345 mechanisms, or activities described above to the Smart Grid information system.  
346

347 Table 2, depicts the assessment objective that corresponds with the sample NISTIR 7628  
348 high-level security requirement, SG.MP-3.

349 **Table 2. SG.MP-3, Media Marking Assessment Objective**

350 **Assessment Objective: SG. MP-3.1**

Determine if:

- (i) the organization documents the storage requirements of stored media;
- (ii) the organization physically manages Smart Grid information system media within protected areas;
- (iii) the organization physically stores Smart Grid information system media within protected areas.

351

### 352 **2.3 Assessment Methods**

353 The assessment methods consist of examine, interview, and test, and define the nature of  
354 the assessor actions. Listed below is a brief description of each type of assessment method:  
355

- 356 • The **examine** method is the process of reviewing, inspecting, observing, studying, or  
357 analyzing one or more assessment objects (i.e., specifications, mechanisms, or  
358 activities). The purpose of the examine method is to facilitate assessor  
359 understanding, achieve clarification, or obtain evidence.
- 360 • The **interview** method is the process of conducting discussions with individuals or  
361 groups of individuals within an organization to facilitate assessor understanding,  
362 achieve clarification, or obtain evidence.
- 363 • The **test** method is the process of exercising one or more assessment objects (i.e.,  
364 activities or mechanisms) under specified conditions to compare actual with  
365 expected behavior.  
366

367 In all three assessment methods, the results are used to make specific determinations,  
368 thereby achieving the objectives for the assessment procedure. Appendix A displays the  
369 definitions of the assessment methods provided by NIST SP 800-53A and adopted for the  
370 NISTIR 7628 assessment process. Table 3, illustrates the corresponding assessment

---

<sup>9</sup> Mechanisms also include physical protection devices associated with a Smart Grid information system (e.g., locks, keypads, security cameras, fire protection devices, fireproof safes, etc.).

371 methods for the sample NISTIR 7628 high-level security requirement and assessment  
 372 objective.

373  
 374

**Table 3. SG.MP-3, Media Marking Assessment Method**

<b>SG.MP-3.1</b>	<p><b>Assessment Objective:</b></p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization documents the storage requirements of stored media;</i></li> <li><i>(ii) the organization physically manages Smart Grid information system media within protected areas;</i></li> <li><i>(iii) the organization physically stores Smart Grid information system media within protected areas.</i></li> </ul> <p><b>Potential Assessment Methods and Objects:</b></p> <p><b>Examine:</b> [SELECT FROM: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and information system output; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Organizational personnel with information system media protection and marking responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Automated mechanisms supporting removable media marking; Media checking process for markings on removable media; Removable media].</p>
------------------	--

375 Each of the assessment methods described has a set of associated attributes, depth and  
 376 coverage, which help define the expected level of effort needed to carry out the assessment.  
 377 These attributes are hierarchical in nature, providing the means to define the assessment  
 378 rigor and scope for the increased assurance needed for higher impact level Smart Grid  
 379 information systems.  
 380

- 381
- 382 • The **depth** attribute addresses the rigor of and level of detail in the examination,  
 383 interview, and testing processes. The depth attribute is expressed using the values  
 384 of generalized, focused, and detailed.
  - 385 • The **coverage** attribute addresses the scope or breadth of the examination,  
 386 interview, and testing processes including the number and type of specifications,  
 387 mechanisms, and activities to be examined or tested and the number and types of  
 388 individuals to be interviewed. The coverage attribute is expressed using the values  
 389 representative, specific, and comprehensive.

390

391 Within the NISTIR 7628, each of the Smart Grid information system impact levels (i.e., low,  
 392 moderate, and high) has an associated set of minimum assurance requirements. Based on  
 393 the assurance requirements, security requirement developers and implementers can carry  
 394 out required activities as an inherent part of developing or implementing the requirement,  
 395 thereby producing the necessary requirement documentation, conducting essential

396 analyses, and defining actions that must be performed during operation.<sup>10</sup> The purpose of  
397 these activities is to provide increased grounds for confidence that the security  
398 requirements are implemented correctly, operating as intended, and producing the desired  
399 outcome.

400  
401 The minimum assurance requirements in the NISTIR 7628 help to establish an appropriate  
402 set of expectations for assessors when conducting the security requirement assessments.  
403 The assessment expectations are based on a Smart Grid information systems impact level –  
404 low, moderate, or high – for a range of assessment objects including specifications,  
405 activities, and mechanisms.

406  
407 An organization should tailor the assessment procedures to match the characteristics of the  
408 Smart Grid information system under assessment. The tailoring process provides  
409 organizations with the flexibility needed to avoid security assessment approaches that are  
410 unnecessarily extensive or more rigorous than necessary. Supplementation involves  
411 adding assessment procedures or assessment details to adequately meet the organization’s  
412 risk management needs (e.g., adding assessment objectives or adding organization-specific  
413 details such as system/platform-specific information for selected security requirements).  
414 Supplementation decisions are left to the discretion of the organization in order to  
415 maximize flexibility in developing security assessment plans<sup>11</sup> when applying the results of  
416 risk assessments in determining the extent, rigor, and level of intensity of the assessments.  
417 While flexibility continues to be an important factor in developing security assessment  
418 plans, consistency of assessments is also an important consideration.

419  
420  
421

---

<sup>10</sup> In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security requirements within a Smart Grid information system. This may include, for example, hardware and software vendors providing the requirements, contractors implementing the requirements, or organizational personnel such as Smart Grid information system owners, system security officers, system and network administrators, or other individuals with security responsibility for the Smart Grid information system.

<sup>11</sup> See Chapter 3 for information on assessment plan development.

### 422 **3. Security Assessment Process**

423 This chapter describes the process of assessing the security requirements in Smart Grid  
424 information systems including: i) the activities carried out by organizations and assessors  
425 to prepare for security requirement assessments, ii) the development of security  
426 assessment plans, iii) the conduct of security requirement assessments and the analysis,  
427 documentation and reporting of assessment results, and iv) post-assessment report  
428 analysis and follow-on activities carried out by organizations.  
429

430 The output and end result of the security requirement assessment is the security  
431 assessment report, which documents the assurance cases<sup>12</sup> for the Smart Grid information  
432 system. The assessment findings in the security assessment report provide information  
433 that informs the organization's risk management processes about the validity of their  
434 implementation of their security plan.

#### 435 **3.1 Preparing for Security Requirement Assessments**

436 Successful security requirement assessments depend on the cooperation and collaboration  
437 among all parties having a vested interest in the organization's information security  
438 posture, including Smart Grid information system owners and senior organizational  
439 leadership. Establishing an appropriate set of expectations before, during and after the  
440 assessment is paramount to achieving an acceptable outcome—that is, producing  
441 information necessary to help organizational officials make a credible, risk-based decision  
442 on whether to place a Smart Grid information system into operation, continue its operation,  
443 or determine which mitigations to implement first. Thorough preparation by the  
444 organization and the assessors is an important aspect of conducting effective security  
445 requirement assessments. Preparatory activities address a range of issues relating to the  
446 cost, schedule, and performance of the assessment.  
447

448 An organization's key activities, when preparing for a security requirement assessment,  
449 include:

- 450
- 451 • Ensuring that appropriate policies covering security requirement assessments are
- 452 in place and understood by all affected organizational elements;
- 453 • Ensuring that security requirements have been assigned to appropriate
- 454 organizational entities for development and implementation;
- 455 • Establishing the objective and scope of the security requirement assessment (i.e.,
- 456 the *purpose* of the assessment and what is being assessed);
- 457 • Notifying key organizational officials of the impending assessment and allocating
- 458 necessary resources to carry out the assessment;
- 459 • Establishing appropriate communication channels among organizational officials
- 460 having an interest in the assessment;

---

<sup>12</sup> An assurance case is a structured set of arguments and a body of evidence showing that a Smart Grid system satisfies specific claims with respect to a given quality attribute.

- 461 • Establishing time frames for completing the assessment and key milestone decision  
462 points required by the organization to effectively manage the assessment;
- 463 • Identifying and selecting a competent assessor/assessment team that will be  
464 responsible for conducting the assessment, considering issues of assessor  
465 independence;
- 466 • Collecting artifacts to provide the assessor/assessment team. Examples of artifacts  
467 include policies, procedures, plans, specifications, designs, records,  
468 administrator/operator manuals, Smart Grid information system documentation,  
469 interconnection agreements, previous assessment results, etc.; and
- 470 • Establishing a mechanism between the organization and the assessor to minimize  
471 ambiguities or misunderstandings about security requirement implementation or  
472 security requirement weaknesses/deficiencies identified during the assessment.  
473

474 Assessors' key activities, when preparing for a security requirement assessment, include:  
475

- 476 • Obtaining a general understanding of the organization's operation (including  
477 mission, functions, and business processes) and how the Smart Grid information  
478 system to be assessed supports those organizational operations;
- 479 • Obtaining an understanding of the structure of the information system (i.e., system  
480 architecture);
- 481 • Obtaining a thorough understanding of the security requirements being assessed;
- 482 • Establishing appropriate organizational points of contact needed to carry out the  
483 assessment;
- 484 • Obtaining artifacts needed for the assessment (see the example artifacts listed  
485 above for the organization's activities);
- 486 • Obtaining previous assessment results that may be appropriately reused for the  
487 current assessment;
- 488 • Meeting with appropriate organizational officials to ensure common understanding  
489 for assessment objectives and the proposed rigor and scope of the assessment; and  
490 • Developing a security assessment plan<sup>13</sup>.

### 491 **3.2 Developing Security Assessment Plans**

492 The security assessment plan provides the objectives for the security requirement  
493 assessment and a detailed roadmap of how to conduct such an assessment.  
494

495 Assessors should consider the following steps when developing plans to assess the security  
496 requirements for Smart Grid information systems:  
497

- 498 • Determine which security requirements/requirement enhancements are to be  
499 included in the assessment based on the contents of the security plan and the  
500 purpose/scope of the assessment (i.e., where "scope" refers to a complete or partial  
501 assessment);

---

<sup>13</sup> Additional guidance on preparing for cybersecurity requirement assessments can be found in section 3.1 of NIST SP 800-53A.

- 502 • Select the appropriate assessment procedures to be used during the assessment
- 503 based on the security requirements and requirement enhancements;
- 504 • Tailor the selected assessment procedures for the Smart Grid information system
- 505 impact level and organization's operating environment;
- 506 • Optimize the assessment procedures to reduce duplication of effort and provide
- 507 cost-effective assessment solutions; and
- 508 • Finalize the assessment plan and obtain the necessary approvals to execute the plan.

### 509 **3.2.1 Determine which security requirements are to be assessed**

510 The cybersecurity system plan provides an overview of the security requirements for the  
511 Smart Grid information system and describes the security requirements to be assessed.  
512 The assessor starts with the security requirements described in the security plan and  
513 considers the purpose of the assessment. A security requirement assessment can be either  
514 a complete or partial assessment of the security requirements implemented in the Smart  
515 Grid information system. Complete assessments address all implemented security  
516 requirements.

517  
518 For partial assessments, Smart Grid information system owners collaborate with  
519 organizational officials (e.g., chief information security officers, asset owners,  
520 mission/information owners, and executive management) to determine which security  
521 requirements are to be assessed. The selection of the security requirements to assess  
522 depends on the Smart Grid information system owner and the organization to ensure that  
523 requirements with greater volatility or importance to the organization are assessed more  
524 frequently, and requirement implementations that have changed since the last assessment  
525 are reevaluated.<sup>14</sup>

### 526 **3.2.2 Select appropriate procedures to assess the security requirements**

527 Appendix B provides an assessment procedure for each security requirement and  
528 requirement enhancement in the NISTIR 7628. For each security requirement and  
529 requirement enhancement in the security plan to be included in the assessment, assessors  
530 select the corresponding assessment procedure from the spreadsheet.

### 531 **3.2.3 Tailor assessment procedures for specific operating environments**

532 The assessment procedures listed in Appendix B are tailored to meet specific  
533 organizational needs, in a manner similar to how the security requirements from the  
534 NISTIR 7628 are tailored for the organization's mission, business functions, characteristics  
535 of the Smart Grid information system and operating environment,. Assessment procedures  
536 can be tailored by:

- 537
- 538 • Selecting the assessment methods and objects needed to satisfy assessment
- 539 objectives and most cost-effectively make appropriate determinations;

---

<sup>14</sup> NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidance on continuous monitoring as part of the risk management process.

- 540 • Selecting the appropriate depth and coverage attribute values defines the scope and  
541 rigor of the assessment to be performed;
- 542 • Eliminating assessment procedures for common security requirements if those  
543 requirements have been assessed by another documented assessment process;
- 544 • Developing Smart Grid information system-specific assessment procedures;
- 545 • Incorporating assessment results from previous assessments, where the results  
546 deemed are applicable; and
- 547 • Making appropriate adjustments in assessment procedures to be able to obtain the  
548 requisite assessment evidence from external providers.

### 549 **3.2.4 Optimize selected assessment procedures to ensure maximum efficiency**

550 Assessors have a great deal of flexibility to select assessment methods in order to develop a  
551 security assessment plan provides the necessary information for an organization to  
552 determine the validity of their implementation of their security plan. Combining and  
553 consolidating assessment procedures is one area where this flexibility can be applied.  
554 During the assessment of a Smart Grid information system, assessment methods are  
555 applied numerous times to a variety of assessment objects within a particular family of  
556 security requirements. To save time, reduce assessment costs, and maximize the usefulness  
557 of assessment results, assessors should review the selected assessment procedures for the  
558 security requirement families and combine or consolidate the procedures (or parts of  
559 procedures) whenever possible or practicable.

### 560 **3.2.5 Finalize security assessment plan and obtain approval to execute plan**

561 After completing the preceding steps, the security assessment plan is finalized and the  
562 schedule is established including key milestones for the assessment process. Once the  
563 security assessment plan is completed, the plan is reviewed and approved by appropriate  
564 organizational officials to ensure that the plan is complete, consistent with the security  
565 objectives of the organization and the organization's assessment of risk, and cost-effective  
566 with regard to the resources allocated for the assessment.

## 567 **3.3 *Conducting Security Requirement Assessments***

568 After the security assessment plan is approved by the organization, the assessor executes  
569 the plan in accordance with the agreed-upon milestones and schedule. Assessment  
570 objectives are achieved by applying the designated assessment methods to selected  
571 assessment objects and compiling/producing the information necessary to make the  
572 determination associated with each assessment objective.

573  
574 Each determination statement contained within an assessment procedure executed by an  
575 assessor produces an associated finding, even though findings may be expressed differently  
576 by across assessor organizations. In general, the findings can be expressed as one of the  
577 following:

- 578  
579 • **Satisfied (S).** The assessment information obtained (i.e., evidence collected)  
580 indicates that the assessment objective for the requirement has been met producing  
581 a fully acceptable result.

- 582 • **Other than satisfied (O).** The assessment information obtained indicates potential  
583 anomalies in the operation or implementation of the requirement that may need to  
584 be addressed by the organization. A finding of other than satisfied may also indicate  
585 that for reasons specified in the assessment report, the assessor was unable to  
586 obtain sufficient information to make the particular determination called for in the  
587 determination statement.  
588

589 However, the assessor organization may have a more robust lexicon for expressing their  
590 findings.

591  
592 The Smart Grid information system owner relies on the assessor's security expertise and  
593 technical judgment to: (i) assess the security requirements in the Smart Grid information  
594 system; and (ii) provide specific recommendations on how to correct weaknesses or  
595 deficiencies in the requirements and reduce or eliminate identified vulnerabilities. The  
596 assessor provides this information to the Smart Grid information system owner in the  
597 initial (draft) security assessment report. If there are specific opportunities to correct  
598 weaknesses or deficiencies in the security requirements or to correct/clarify  
599 misunderstandings or interpretations of assessment results, then the system owner may  
600 choose to act on selected recommendations before the security assessment report is  
601 finalized. Security requirements modified, enhanced, or added during this process should  
602 be reassessed by the assessor prior to the production of the final security assessment  
603 report. The delivery of the final assessment report to the Smart Grid information system  
604 owner marks the official end of the security requirement assessment.

### 605 ***3.4 Analyzing Security Assessment Report Results***

606 Since results of the security requirement assessment ultimately influence the content of the  
607 security plan, the Smart Grid information system owner reviews the security assessment  
608 report. Then with the concurrence of designated organizational officials, the Smart Grid  
609 information system owner determines the appropriate steps required to correct  
610 weaknesses and deficiencies identified during the assessment. By using the tags of satisfied  
611 and other than satisfied, the reporting format for the assessment findings provides  
612 visibility for organizational officials into specific weaknesses and deficiencies in the Smart  
613 Grid information system and facilitates a disciplined and structured approach to mitigating  
614 risks in accordance with organizational priorities.  
615

616 Senior leadership involvement in the mitigation process is necessary to ensure that the  
617 organization's resources are effectively allocated in accordance with organizational  
618 priorities. Leadership first provides resources to the Smart Grid information systems that  
619 are: i) supporting the most critical and sensitive missions for the organization or ii)  
620 correcting the deficiencies that pose the greatest degree of risk. Ultimately, the assessment  
621 findings and any subsequent mitigation actions initiated by the Smart Grid information  
622 system owner in collaboration with designated organizational officials trigger updates to  
623 the risk assessment and the security plan.  
624

625 Figure 1 provides an overview of the security requirement assessment process, including the activities carried out during pre-  
 626 assessment, assessment, and post-assessment.  
 627

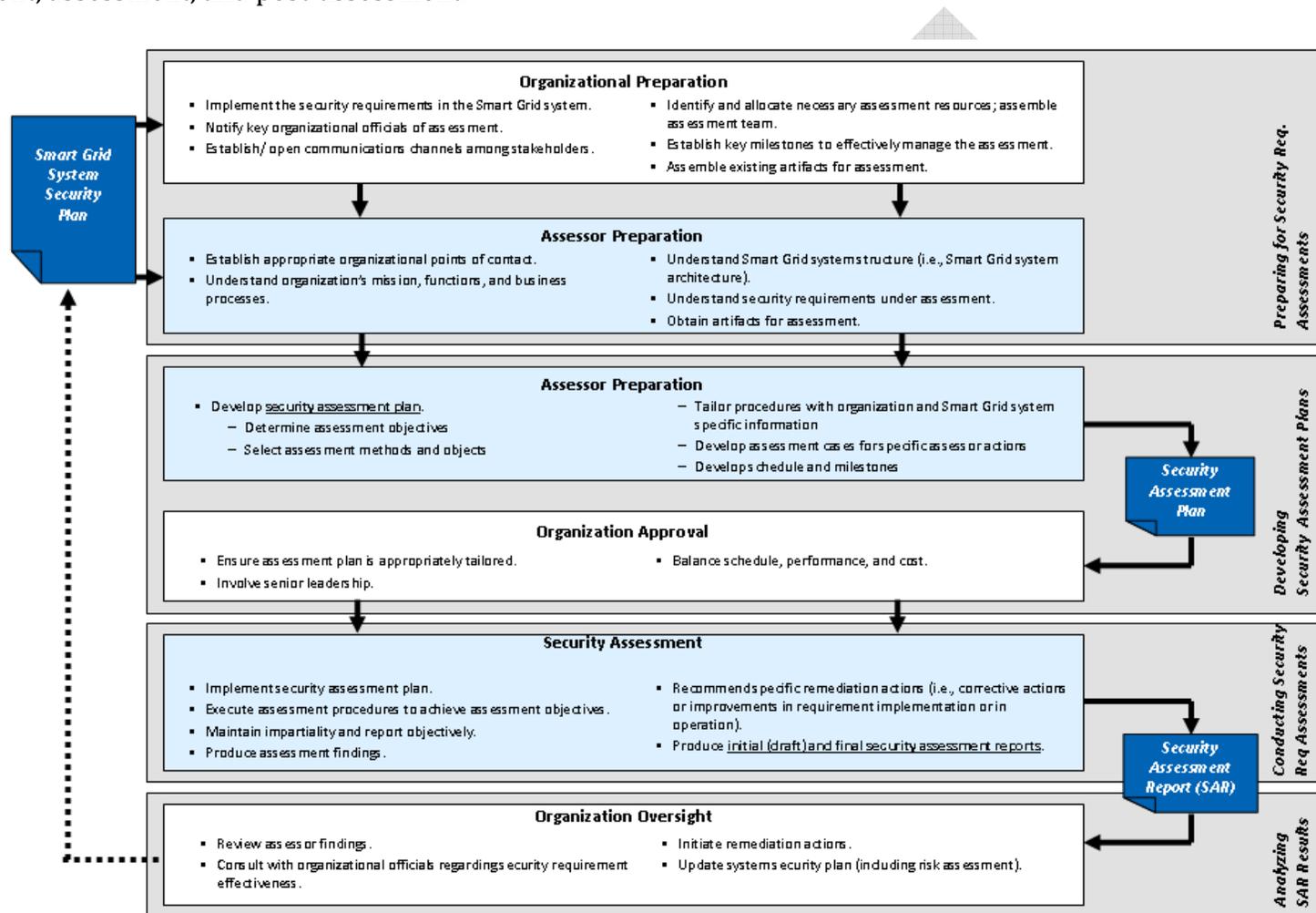


Figure 1. Smart Grid Security Requirement Assessment Process Overview <sup>15</sup>

<sup>15</sup> This figure was adapted from Figure 1-Security Control Assessment Process Overview of NIST SP 800-53A: *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans* (See <http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf>).

628  
629

630 **4. Revision History**

631  
632 SGIP Document Number: CSWG-TC-001, Version 0.8  
633

634 **THIS IS NOT A NIST DOCUMENT**  
635

Rev. Number	Date	Author/Editor	Summary of Revisions
0.3	8/15/2011	CSWG TCC	Initial document
0.4 - 0.8	09/15/2011 - 11/21/2011	CSWG Management Team	Comments and updates

636

637 **5. Contributors**

638 Thank you to the following members of the CSWG and CSWG Security Testing and  
639 Certification Subgroup for their contributions in developing this document:

- 640 • Mike Ahmadi
- 641 • Sandy Bacik
- 642 • Richard Bockenek
- 643 • James Foti
- 644 • Nelson Hastings
- 645 • Michaela Iorga
- 646 • Stan Kladko
- 647 • Victoria Yan Pillitteri
- 648 • Scott Shorter
- 649 • Marianne Swanson

650

651 **Appendix A – NIST SP800-53A Assessment Method Definitions**

ASSESSMENT METHOD	ASSESSMENT OBJECTS	DEFINITION	SUPPLEMENTAL GUIDANCE
Examine	<p>Specifications (e.g., policies, plans, procedures, system requirements, designs)</p> <p>Mechanisms (e.g., functionality implemented in hardware, software, firmware)</p> <p>Activities (e.g., system operations, administration, management, exercises)</p>	<p>The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.</p>	<p>Typical assessor actions may include, for example:</p> <ul style="list-style-type: none"> <li>• reviewing information security policies, plans, and procedures;</li> <li>• analyzing system design documentation and interface specifications;</li> <li>• observing system backup operations, reviewing the results of contingency plan exercises;</li> <li>• observing incident response activities;</li> <li>• studying technical manuals and user/administrator guides;</li> <li>• checking, studying, or observing the operation of an information technology mechanism in the Smart Grid information system hardware/software; or</li> <li>• checking, studying, or observing physical security measures related to the operation of a Smart Grid information system.</li> </ul>
Interview	<p>Individuals or groups of individuals.</p>	<p>The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.</p>	<p>Typical assessor actions may include, for example:</p> <ul style="list-style-type: none"> <li>• interviewing agency heads,</li> <li>• chief information officers,</li> <li>• senior agency information security officers,</li> <li>• authorizing officials,</li> <li>• information owners,</li> <li>• Smart Grid information system and mission owners,</li> <li>• Smart Grid information system security officers,</li> <li>• Smart Grid information system security managers,</li> <li>• personnel officers,</li> <li>• human resource managers,</li> <li>• facilities managers,</li> <li>• training officers,</li> <li>• Smart Grid information system operators,</li> <li>• network and system administrators,</li> <li>• site managers,</li> <li>• physical security officers, and</li> <li>• users.</li> </ul>
Test	<p>Mechanisms (e.g., hardware, software, firmware)</p> <p>Activities (e.g., system operations, administration, management, exercises)</p>	<p>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.</p>	<p>Typical assessor actions may include, for example:</p> <ul style="list-style-type: none"> <li>• testing access control, identification and authentication, and audit mechanisms;</li> <li>• testing security configuration settings;</li> <li>• testing physical access control devices; conducting penetration testing of key Smart Grid information system components;</li> <li>• testing Smart Grid information system backup operations;</li> <li>• testing incident response capability; and</li> <li>• exercising contingency planning capability.</li> </ul>

652

653 **Appendix B – Assessment Procedures Catalog**

654

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
<b>Access Control (SG.AC)</b>				
SG.AC-1	Access Control Policy and Procedures	SG.AC-1.1 Determine if: (i) the organization develops and implements a documented access control policy; (ii) the access control policy addresses access control as it related to protecting the organization’s personnel and assets and the following: a) purpose / objective b) scope c) roles and responsibilities e) coordination among organizational entities, and compliance; (iii) the access control policy addresses the scope to include all organizational staff, contractors, and third parties; (iv) the organization develops and implements the access control procedures; (v) the organization reviews and updates the access control procedures; (vi) management commitment ensures compliance with the organization’s access control; (vii) the access control policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (viii) the access control procedures facilitate implementation of the access control security policy.  SG.AC-1.2 Determine if: (i) the organization defines the frequency of access control policy and procedures reviews/updates; (ii) the organization reviews/updates the access control policy and procedures in accordance with the organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.AC-2	Remote Access Policy and Procedures	SG.AC-2.1 Determine if: (i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the Smart Grid information system is allowed; (ii) the organization documents the allowed remote access to the Smart Grid information system; (iii) the organization authorizes remote access to the Smart Grid information system prior to connection; (iv) the organization enforces requirements for remote connections	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		to Smart Grid information systems.  SG.AC-2.2 Determine if: (i) the organization defines managed access control points for remote access to the Smart Grid information system; and (ii) the Smart Grid information system controls all remote accesses through a limited number of managed access control points.		
SG.AC-3	Account Management	SG.AC-3.1 Determine if: (i) the organization manages Smart Grid information system accounts, including a) authorizing b) establishing c) activating d) modifying e) reviewing f) disabling g) removing accounts; (ii) the organization requires management approval prior to establishing accounts; (iii) the organization documents management approval prior to establishing accounts; (iv) the organization documents account types; (v) the organization documents access rights; (vi) the organization documents privileges.  SG.AC-3.2 Determine if the organization reviews accounts in accordance with the organization-defined frequency.  SG.AC-3.3 Determine if: (i) the organizations notified account managers when Smart Grid information system users are terminated; (ii) the organizations notified account managers when Smart Grid information system users are transferred; (iii) the organizations notified account managers when Smart Grid information system usage changes.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with access control and remote access responsibilities].  Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].
SG.AC-4	Access Enforcement	SG.AC-4.1 Determine if the Smart Grid information system enforces assigned authorizations for controlling access to the system in accordance with the organizational defined policy.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				<p>transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with access control and remote access responsibilities].</p> <p>Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].</p>
SG.AC-5	Information Flow Enforcement	<p>SG.AC-5.1 Determine if:</p> <p>(i) the Smart Grid information system enforces assigned authorizations for controlling the flow of information within the Smart Grid information system in accordance with the organizational policy;</p> <p>(ii) the Smart Grid information system enforces assigned authorizations for controlling the flow of information between interconnected systems in accordance with the organizational policy.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with access control and remote access responsibilities].</p> <p>Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].</p>
SG.AC-6	Separation of Duties	<p>SG.AC-6.1 Determine if:</p> <p>(i) the organization establishes divisions of responsibility as needed to eliminate conflicts of interest in the responsibilities and duties of individuals;</p> <p>(ii) the organization documents divisions of responsibility duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals;</p> <p>(iii) the organization establishes separation of duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals;</p>	Examine, Test	<p>Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>(iv) the organization documents separation of duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.</p> <p>SG.AC-6.2 Determine if the organization enforces separation of smart grid functions through assigned access authorizations.</p> <p>SG.AC-6.3 Determine if the organization restricts security functions to an organizational defined minimum amount of users necessary to ensure the security of the Smart Grid information system.</p>		<p>relevant documents or records].</p> <p>Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].</p>
SG.AC-7	Least Privilege	<p>SG.AC-7.1 Determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.</p> <p>SG.AC-7.2 Determine if the organization configures the Smart Grid information system to enforce the most restrictive set of rights/privileges or accesses needed by users.</p>	Examine, Test	<p>Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records].</p> <p>Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].</p>
SG.AC-8	Unsuccessful Login Attempts	<p>SG.AC-8.1 Determine if:</p> <p>(i) the organization defines a limit of consecutive invalid access attempts by a user during an organization-defined time period;</p> <p>(ii) the organization enforces the limit of consecutive invalid access attempts by a user during an organization-defined time period;</p> <p>(iii) the organization defines the time period for consecutive invalid access attempts by a user.</p>	Examine, Test	<p>Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records].</p> <p>Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports,</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				automated mechanisms implementing account management functions].
SG.AC-9	Smart Grid information system Use Notification	SG.AC-9.1 Determine if: (i) the organization defines a system use notification message / banner for security and privacy for the Smart Grid information system consistent with applicable laws, directives, policies, regulations, standards, and guidance; (ii) the organization documents a system use notification message / banner for security and privacy for the Smart Grid information system; (iii) the organization approves a system use notification message / banner for security and privacy for the Smart Grid information system; (iv) the Smart Grid information system displays an approved system use notification message / banner for security and privacy before granting Smart Grid information system access.	Examine, Test	Examine: [SELECT FROM: Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of Smart Grid information system use notification messages or banners; Smart Grid information system notification messages; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records for user acceptance of notification message or banner; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing the access control policy for system use notification].
SG.AC-10	Previous Logon Notification	SG.AC-10.1 Determine if: (i) the Smart Grid information system, upon successful logon, displays a) the date of the last logon; b) the time of the last logon; c) the number of unsuccessful logon attempts since the last successful logon.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing previous logon notification; Smart Grid information system configuration settings and associated documentation; Smart Grid information system notification messages; Smart Grid information system design documentation; Smart Grid information system design documentation; Smart Grid information system audit records; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing the access control policy for previous logon notification].
SG.AC-11	Concurrent Session Control	SG.AC-11.1 Determine if: (i) the organization defines the limit of concurrent sessions for any user on the Smart Grid information system; (ii) the organization enforces the limit of concurrent sessions for any user on the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing previous logon notification; Smart Grid information system configuration settings and associated documentation; Smart Grid information system notification messages; Smart Grid information system design documentation; Smart Grid information system design documentation; Smart Grid information system audit records; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing the access control policy for concurrent session control].
SG.AC-12	Session Lock	SG.AC-12.1 Determine if: (i) the organization defines the time period of user inactivity after which the Smart Grid information system initiates a session lock; (ii) the organization enforces the time period of user inactivity after which the Smart Grid information system initiates a session lock of receiving a request from a user.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing session lock; display screen with session lock activated; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; security plan; other relevant documents or records].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.AC-12.2 Determine if the Smart Grid information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.		Test: [SELECT FROM: Automated mechanisms implementing the access control policy for session lock; Smart Grid information system session lock mechanisms].
SG.AC-13	Remote Session Termination	SG.AC-13.1 Determine if: (i) the organization defines the time period of remote user inactivity after which the Smart Grid information system initiates a session lock; (ii) the organization enforces the time period of remote user inactivity after which the Smart Grid information system initiates a session lock of receiving a request from a user; (iii) the Smart Grid information system terminates a remote session at the end of the remote session or after the organizationally defined remote access inactivity period.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing session timing and termination; display screen with session lock activated; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; security plan; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing the access control policy for session lock; Smart Grid information system session timing and termination mechanisms].
SG.AC-14	Permitted Actions without Identification or Authentication	SG.AC-14.1 Determine if: (i) the organization identifies specific user actions that can be performed on the Smart Grid information system without identification or authentication; (ii) the organization documents specific user actions that can be performed on the Smart Grid information system without identification or authentication.  SG.AC-14.2 Determine if the organization 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.  SG.AC-14.3 Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing permitted actions without identification and authentication; Smart Grid information system configuration settings and associated documentation; security plan; list of Smart Grid information system actions that can be performed without identification and authentication; Smart Grid information system audit records; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing the access control policy for sessions without identity or with unauthenticated access; Smart Grid information system session lock mechanisms].
SG.AC-15	Remote Access	SG.AC-15.1 Determine if: (i) the organization authorizes remote access to the Smart Grid information system for all allowed methods of remote access; (ii) the organization monitors remote access to the Smart Grid information system for all allowed methods of remote access; (iii) the organization controls remote access to the Smart Grid information system for all allowed methods of remote access.  SG.AC-15.2 Determine if:	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the Smart Grid information system; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; security plan; list of networking protocols deemed to be not secure; other relevant documents or records].  Test: [SELECT FROM: Remote access methods for the Smart Grid information system; Automated mechanisms implementing the access control policy for remote access; Automated mechanisms disabling networking protocols deemed to be not

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>(i) the organization authenticates remote access;                      (ii) the organization uses cryptography to protect the confidentiality and integrity of remote access sessions;</p> <p>SG.AC-15.3                      Determine if:                      (i) the organization defines a limited number of managed access control points for remote access to the Smart Grid information system; and                      (ii) the Smart Grid information system controls all remote accesses through a limited number of managed access control points.</p> <p>SG.AC-15.4                      Determine if:                      (i) the organization defines the protection of wireless access to the Smart Grid information system by using authentication and encryption;                      (ii) the Smart Grid information system uses authentication and encryption to protect wireless access.</p> <p>SG.AC-15.5                      Determine if:                      (i) the organization monitors for unauthorized remote connections to the Smart Grid information system and takes appropriate action if an unauthorized connection is discovered;                      (ii) the organization defines a frequency for scanning wireless access points;                      (iii) the organization defines actions for unauthorized wireless connections to the Smart Grid information system;                      (iv) the organization enforces the actions for unauthorized wireless connections to the Smart Grid information system.</p>		secure].
SG.AC-16	Wireless Access Restrictions	<p>SG.AC-16.1                      Determine if:                      (i) the organization establishes use restrictions and implementation guidance for wireless technologies;                      (ii) the organization authorizes wireless access to the Smart Grid information system;                      (iii) the organization monitors wireless access to the Smart Grid information system;                      (iv) the organization manages wireless access to the Smart Grid information system.</p>	Examine, Test	<p>Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the Smart Grid information system; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; security plan; list of networking protocols deemed to be not secure; policy and procedures addressing wireless access and wireless access points; other relevant documents or records].</p> <p>Test: [SELECT FROM: Remote access methods for the Smart Grid information system; Automated mechanisms implementing the access control policy for remote access; Automated mechanisms disabling networking protocols deemed to be not secure; wireless scanning assessments].</p>
SG.AC-17	Access Control for	SG.AC-17.1	Examine,	Examine: [SELECT FROM: Access control policy; procedures

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
	Portable and Mobile Devices	<p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization establishes usage restrictions for organization-controlled portable and mobile devices, including the use of writeable, removable media and personally owned removable media;</li> <li>(ii) the organization establishes implementation guidance for organization-controlled portable and mobile devices, including the use of writeable, removable media and personally owned removable media.</li> </ul> <p>SG.AC-17.2 Determine if the organization authorizes connections of mobile devices to the Smart Grid information system.</p> <p>SG.AC-17.3 Determine if the organization monitors for unauthorized connections of mobile devices to the Smart Grid information system.</p> <p>SG.AC-17.4 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents requirements for the connection of mobile devices to the Smart Grid information system;</li> <li>(ii) the organization enforces requirements for the connection of mobile devices to the Smart Grid information system.</li> </ul> <p>SG.AC-17.5 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents the use of writable, removable media in Smart Grid information systems;</li> <li>(ii) the organizations controls the use of writable, removable media in Smart Grid information systems.</li> </ul> <p>SG.AC-17.6 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents the use of personally owned removable media in Smart Grid information systems;</li> <li>(ii) the organizations controls the use personally owned removable media in Smart Grid information systems.</li> </ul> <p>SG.AC-17.7 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents the configuration of mobile devices assigned to individual travelling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures;</li> </ul>	Test	<p>addressing access control for portable and mobile devices; evidentiary documentation for random inspections of mobile devices; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing access control policy for portable and mobile devices; automated mechanisms prohibiting the use of internal or external modems or wireless interfaces with mobile devices].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>(ii) the organization maintains the organizationally defined configured mobile devices to be assigned to individual travelling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures;</p> <p>(iii) the organization provides organizationally defined configured mobile devices to be assigned to individual travel to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures.</p> <p>SG.AC-17.8 Determine if:</p> <p>(i) the organization documents measures of mobile returning from individual travelling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures;</p> <p>(i) the organization enforces measures of mobile returning from individual travelling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures.</p>		
SG.AC-18	Use of External Information Control Systems	<p>SG.AC-18.1 Determine if the organizations documents terms and conditions for authorized individual to access the Smart Grid information system from an external Smart Grid information system.</p> <p>SG.AC-18.2 Determine if the organizations documents terms and conditions for authorized individual to</p> <ul style="list-style-type: none"> <li>a) process organization-controlled information using an external Smart Grid information system;</li> <li>b) store organization-controlled information using an external Smart Grid information system;</li> <li>c) transmit organization-controlled information using an external Smart Grid information system.</li> </ul> <p>SG.AC-18.3 Determine if:</p> <p>(i) the organizations documents restrictions on authorized individual with regard to the use of organization-controlled removable media on external Smart Grid information systems;</p> <p>(ii) the organizations enforces restrictions on authorized individual with regard to the use of organization-controlled removable media on external Smart Grid information systems.</p>	Examine, Test	<p>Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the Smart Grid information system; list of mediation vehicles for allowing public access to the organization's internal networks; Smart Grid information system design documentation; boundary protection hardware and software; Smart Grid information system configuration settings and associated documentation; communications and network traffic monitoring logs; enterprise security architecture documentation; other relevant documents or records].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing boundary protection capability within the Smart Grid information system; Automated mechanisms implementing access controls for public access to the organization's internal networks].</p>
SG.AC-19	Control System Access Restrictions	<p>SG.AC-19.1 Determine if:</p> <p>(i) the organization documents mechanisms in the design and implementation of a Smart Grid information system to restrict</p>	Examine, Test	<p>Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the Smart Grid information system; list of mediation vehicles for allowing public access to</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		access to the Smart Grid information system from the organization's enterprise network; (ii) the organization implements 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; (iii) the organization enforces 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.		the organization's internal networks; Smart Grid information system design documentation; boundary protection hardware and software; Smart Grid information system configuration settings and associated documentation; communications and network traffic monitoring logs; enterprise security architecture documentation; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing boundary protection capability within the Smart Grid information system; Automated mechanisms implementing access controls for public access to the organization's internal networks].
SG.AC-20	Publicly Accessible Content	SG.AC-20.1 Determine if the organization designates individuals authorized to post information onto an organizational Smart Grid information system that is publicly accessible.  SG.AC-20.2 Determine if the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.  SG.AC-20.3 Determine if the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational Smart Grid information system.  SG.AC-20.4 Determine if the organization reviews the content on the publicly accessible organizational Smart Grid information system for nonpublic information on an organization-defined frequency.  SG.AC-20.5 Determine if the organization removes nonpublic information from the publicly accessible organizational Smart Grid information system, if discovered.	Examine, Interview	Examine: [SELECT FROM: Public information policy; Social media policy; procedures for posting publicly available information; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for posting and maintaining public content].
SG.AC-21	Passwords	SG.AC-21.1 Determine if: (i) the organization develops policies and procedures for Smart Grid information system users concerning the generation and use of passwords; (ii) the organization implements policies and procedures for Smart Grid information system users concerning the generation and use of passwords; (iii) the organization enforces policies and procedures for Smart	Examine, Test	Examine: [SELECT FROM: Password policy; Authentication policy; procedures addressing authentication and password control; security plan; list of active system accounts along with the name of the individual associated with each account and the last time the password has been changed; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires and the last time the password was changed; other relevant documents or records].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>Grid information system users concerning the generation and use of passwords.</p> <p>SG.AC-21.2 Determine if the organizational policies document rules of complexity, based on the criticality level of the Smart Grid information system to be accessed.</p> <p>SG.AC-21.3 Determine if: (i) the organizational policies document rules of passwords shall be changed regularly; (ii) the organizational policies document rules of passwords shall be revoked after an extended period of inactivity.</p>		<p>Test: [SELECT FROM: Automated mechanisms implementing password policy management; automated mechanisms for changing passwords; Automated mechanisms for password expiration].</p>
<b>Awareness and Training (SG.AT)</b>				
SG.AT-1	Awareness and Training Policy and Procedures	<p>SG-AT-1.1 Determine if: (i) the organization develops and implements a documented security awareness and training policy; (ii) the security awareness and training policy addresses security awareness and training as it related to protecting the organization's personnel and assets and the following:     a) purpose / objective     b) scope     c) roles and responsibilities     d) coordination among organizational entities, and compliance; (iii) the security awareness and training policy addresses the scope to include all organizational staff, contractors, and third parties; (iv) the organization develops and implements the security awareness and training procedures; (v) the organization reviews and updates the security awareness and training procedures; (vi) management commitment ensures compliance with the organization's security awareness and training; (vii) the security awareness and training policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (viii) the security awareness and training procedures facilitate implementation of the security awareness and training security policy.</p> <p>SG-AT-1.2 Determine if: (i) the organization defines the frequency of security awareness and training policy and procedures reviews/updates; (ii) the organization reviews/updates the security awareness and</p>	Examine, Interview	<p>Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		training policy and procedures in accordance with the organization-defined frequency.		
SG.AT-2	Security Awareness	SG.AT-2.1 Determine if: (i) the organization provides basic security awareness training to all Smart Grid information system users on an organizational defined frequency; (ii) the organization includes exercises during the security awareness briefings that similar cyber attacks; (iii) the scope of the policy and procedure include organization staff, contractors and third parties; (iv) the security awareness and training materials address the specific requirements of the organization and the Smart Grid information systems to which personnel have authorized access; (v) Smart Grid information system design changes are reviewed for inclusion in the organization awareness training; (vi) Smart Grid information system procedure changes are reviewed for inclusion in the organization awareness training.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel comprising the general Smart Grid information system user community; Organizational personnel that participate in security awareness training].
SG.AT-3	Security Training	SG.AT-3.1 Determine if: (i) the organization provides security training before authorizing access to the Smart Grid information system; (ii) the organization provides security training before performing duties for accessing the Smart Grid information system; (iii) the organization provides security training when required by the Smart Grid information system; (iv) the organization provides security training on an organizational defined frequency; (v) the organization security training includes a) roles and responsibilities b) organizational requirements c) security-related training for assigned duties.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for role-based, security-related training; organizational personnel with significant Smart Grid information system security responsibilities].
SG.AT-4	Security Awareness and Training Records	SG.AT-4.1 Determine if: (i) the organization maintains training records for each user; (ii) the organization maintains training records in accordance with the organization records retention policy.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security training record retention responsibilities].
SG.AT-5	Contact with Security Groups and Associations	SG.AT-5.1 Determine if the organization (i) establishes contact with security group and associations; (ii) maintains contact with security group and associations; (iii) stays up to date on the latest recommended security practices, techniques, and technologies; and (iv) shares current security-related information including threats,	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing Smart Grid information system security knowledge, expertise, and general information; other relevant documents or records].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		vulnerabilities, and incidents.		Interview: [SELECT FROM: Organizational personnel with security responsibilities (e.g., individuals that have contacts with selected groups and associations within the security community)].
SG-AT-6	Security Responsibility Training	SG-AT-6.1 Determine if the organization (i) tests the knowledge of security policies and procedures to ensure knowledge of responsibilities; (ii) maintains a list of security responsibilities for each role; (iii) conducts security responsibility testing on an organizational defined frequency.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; Security training plan; procedures addressing security training plan development and implementation; procedures addressing security plan reviews and updates; other relevant documents or records].  Interview: [SELECT FROM: Organization personnel with security training responsibilities for the Smart Grid information system].
SG-AT-7	Planning Process Training	SG-AT-7.1 Determine if: (i) the organization security training includes the planning process on implementing Smart Grid information systems security plans; (ii) the organization security training includes organization staff, contractors and third parties.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; Security training plan; procedures addressing security training plan development and implementation; procedures addressing security plan reviews and updates; other relevant documents or records].  Interview: [SELECT FROM: Organization personnel with security training responsibilities for the Smart Grid information system].
<b>Audit and Accountability (SG-AU)</b>				
SG-AU-1	Audit and Accountability	SG-AU-1.1 Determine if: (i) the organization develops and implements a documented audit and accountability security policy; (ii) the audit and accountability security policy addresses the objectives, roles, responsibility and scope of the audit and accountability security program; (iii) the organization develops, implements, reviews and updates a audit and accountability procedures; (iv) management commitment ensures compliance with the organization's security; (v) the audit and accountability policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (vi) the audit and accountability procedures facilitate implementation of the audit and accountability security policy.  SG-AU-1.2 Determine if: (i) the organization defines the frequency of audit and accountability security policy reviews/updates; (ii) the organization reviews/updates the audit and accountability security policy in accordance with the organization-defined frequency;	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(iii) the organization defines the frequency of audit and accountability procedures reviews/updates; and (iv) the organization reviews/updates the audit and accountability procedures in accordance with the organization-defined frequency.		
SG.AU-2	Auditable Events	<p>SG.AU-2.1 Determine if: (i) the organization defines the list of events the Smart Grid information system must be capable of auditing based on a risk assessment; (ii) the organization-defined auditable events include execution of privileged functions; (iii) the Smart Grid information system generates audit records for the organization-defined auditable events; (iv) the organization specifies which Smart Grid information system components carry out auditing activities; and (v) the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations.</p> <p>SG.AU-2.2 Determine if: (i) the organization defines the frequency of revising the list of auditable events reviews/updates; and (ii) the organization revises the list of auditable events in accordance with the organization-defined frequency.</p> <p>SG.AU-2.3 (requirements enhancement 1) Determine if the organization audits activities associated with configuration changes to the Smart Grid information system.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Audit and accountability policy; procedures addressing auditable events; security plan; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; list of organization-defined auditable events; auditable events review and update records; Smart Grid information system incident reports; list of Smart Grid information system auditable events; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities; Organizational personnel with responsibilities for monitoring open source information for evidence of unauthorized exfiltration or disclosure].</p>
SG.AU-3	Content of Audit Records	<p>SG.AU-3.1 Determine if: (i) all types of Smart Grid information system audit records record the date and time of the event; (ii) all types of Smart Grid information system audit records record the component where the event occurred; (iii) all types of Smart Grid information system audit records record the type of event; (iv) all types of Smart Grid information system audit records record the identity of the user/subject that caused the event; and (v) all types of Smart Grid information system audit records record the outcome of the event.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; Smart Grid information system audit records; Smart Grid information system incident reports; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities; Organizational personnel with responsibilities for monitoring open source information for evidence of unauthorized exfiltration or disclosure].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing Smart Grid information system auditing of auditable events;</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Smart Grid information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject].
SG.AU-4	Audit Storage Capacity	SG.AU-4.1 Determine if: (i) the organization defines the audit record storage capacity for all Smart Grid information systems; (ii) the organization allocates audit record storage capacity in accordance with the organization defined limits; and (iii) the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit storage capacity; Smart Grid information system design documentation; organization-defined audit record storage capacity for Smart Grid information system components that store audit records; list of organization-defined auditable events; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records].  Test: [SELECT FROM: Audit record storage capacity and related configuration settings].
SG.AU-5	Response to Audit Processing Failures	SG.AU-5.1 Determine if: (i) the organization designates the personnel to be notified in case of an audit processing failure; and (ii) the Smart Grid information system alerts designated organizational officials; (iii) the organization defines in the security plan actions to be taken in the event of an audit processing failure; and (iv) the Smart Grid information systems perform the organization-defined actions when audit processing failure occurs.  SG.AU-5.2 (requirements enhancement 1) Determine if 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.  SG.AU-5.3 (requirements enhancement 2) Determine if: (i) the organization defines what audit failures result in a real-time alert; and (ii) the Smart Grid information system provides a real-time alert for those organization defined audit failure events.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; Smart Grid information system audit records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities; Organizational personnel with responsibilities for monitoring open source information for evidence of unauthorized exfiltration or disclosure].
SG.AU-6	Audit Monitoring, Analysis, and Reporting	SG.AU-6.1 Determine if: (i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity; (ii) the organization investigates suspicious activity or suspected violations; (iii) the organization designates management authorities to whom findings of inappropriate or unusual activities are reported; and	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews / analyses of audit records; procedures for investigating and responding to suspicious activities; threat information documentation from law enforcement, intelligence community, or other sources; Smart Grid information system configuration settings and associated documentation;

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>(iv) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to the designated management authorities.</p> <p>SG.AU-6.2 Determine if organization adjusts the level of audit review, analysis, and reporting within the Smart Grid information system when a change in risk occurs due to organizational operations, organizational assets, or individuals.</p>		<p>integrated analysis of audit records, vulnerability scanning information, performance data, network monitoring information and associated documentation; Smart Grid information system audit records; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; security plan; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities].</p> <p>Test: [SELECT FROM: Smart Grid information system audit review, analysis, and reporting capability; Smart Grid information system capability integrating audit review, analysis, and reporting into an organizational process for investigation and response to suspicious activities; Smart Grid information system capability for centralizing review and analysis of audit records from multiple Smart Grid information system components].</p>
SG.AU-7	Audit Reduction and Report Generation	<p>SG.AU-7.1 Determine if: (i) the Smart Grid information system provides audit reduction capabilities; and (ii) the Smart Grid information system provides report generation tools capabilities.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit reduction and report generation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; Smart Grid information system audit records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities].</p> <p>Test: [SELECT FROM: Audit reduction and report generation capability].</p>
SG.AU-8	Time Stamps	<p>SG.AU-8.1 Determine if all Smart Grid information system components use internal system clocks to generate time stamps in audit records.</p> <p>SG.AU-8.2 (requirement enhancement 1) Determine if: (i) the organization defines a time source for clock synchronization; (ii) the organization defines the frequency for clock synchronization; and (iii) all Smart Grid information system components synchronize their clocks at the organization-defined frequency using an</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Audit and accountability policy; procedures addressing time stamp generation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		organization-defined time source.		Test: [SELECT FROM: Automated mechanisms implementing time stamp generation; Automated mechanisms implementing internal Smart Grid information system clock synchronization].
SG.AU-9	Protection of Audit Information	SG.AU-9.1 Determine if the Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation, Smart Grid information system audit records; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation, system or media storing backups of Smart Grid information system audit records; audit tools; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities].  Test: [SELECT FROM: Automated mechanisms implementing audit information protection; Media storage devices to hold audit records].
SG.AU-10	Audit Record Retention	SG.AU-10.1 Determine if: (i) the organization defines the retention period for audit records generated by the Smart Grid information system; and (ii) the organization retains Smart Grid information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; Smart Grid information system audit records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record retention responsibilities].
SG.AU-11	Conduct and Frequency of Audits	SG.AU-11.1 Determine if: (i) the organization defines the frequency of audits; (ii) the organization conducts audits in accordance with the organization-defined frequency; and (iii) the audits assess conformance to specified security requirements and applicable laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy and procedures; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with audit and accountability responsibilities].
SG.AU-12	Auditor Qualification	SG.AU-12.1 Determine if: (i) the organization's audit program specifies auditor qualifications; (ii) the organization selects auditors that understand the Smart Grid information system and associated operating practices; (iii) the organization selects auditors that understand the risks involved with the audit; (iv) the organization selects auditors that understand the organization cyber security and the Smart Grid information system policy and procedures; and	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy and procedures Auditor job description / qualification document; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with audit and accountability responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(v) the organization selects auditors that are organizationally separated from the administration of the Smart Grid information system.		
SG.AU-13	Audit Tools	SG.AU-13-1 Determine if the organization specifies the rules and conditions of use for audit tools	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit reduction and report generation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; Smart Grid information system audit records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities].
SG.AU-14	Security Policy Compliance	SG.AU-14.1 Determine if the organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.AU-15	Audit Generation	SG.AU-15.1 Determine if: (i) the Smart Grid information system provides audit record generation capability for the selected list of auditable events; (ii) the Smart Grid information system generates audit records for the selected list of auditable events; (iii) the Smart Grid information system allows authorized users to select auditable events at the organization-defined Smart Grid information system components.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit record generation; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record generation responsibilities].
SG.AU-16	Non-Repudiation	SG.AU-16.1 Determine if the Smart Grid information system protects against an individual falsely denying having performed a particular action.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing non-repudiation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record generation responsibilities].  Test: [SELECT FROM: Automated mechanisms implementing non-repudiation capability; Cryptographic mechanisms implementing digital signature capability within the Smart Grid information system].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
<b>Security Assessment and Authorization (SG.CA)</b>				
SG.CA-1	Security Assessment and Authorization Policy and Procedures	<p>SG.CA-1.1 Determine if the organization develops, implements, reviews, and updates on an organizational defined frequency</p> <ul style="list-style-type: none"> <li>a) A documented security assessment and authorization policy that addresses—                             <ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul> </li> <li>b) Procedures to address the implementation of the security assessment and authorization policy and associated security assessment and authorization protection requirements.</li> </ul> <p>SG.CA-1.2 Determine if management commitment ensures compliance with the organization’s security assessment and authorization security policy and other regulatory requirements.</p> <p>SG.CA-1.3 Determine if 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.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>
SG.CA-2	Security Assessments	<p>SG.CA-2.1 Determine if the organization develops a security assessment plan that describes the scope of the assessment including—</p> <ul style="list-style-type: none"> <li>a) security requirements and requirement enhancements under assessment;</li> <li>b) assessment procedures to be used to determine security requirement effectiveness; and</li> <li>c) assessment environment, assessment team, and assessment roles and responsibilities.</li> </ul> <p>SG.CA-2.2 Determine if the organizations assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are</p> <ul style="list-style-type: none"> <li>a) implemented correctly;</li> <li>b) operating as intended;</li> <li>c) producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system.</li> </ul> <p>SG.CA-2.3</p>	Examine, Interview	<p>Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with security assessment responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if the organization produces a security assessment report that documents the results of the assessment.  SG.CA-2.4 Determine if the organization provides the results of the security requirements assessment to a management authority.		
SG.CA-3	Continuous Improvement	SG.CA-3.1 Determine if 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.	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security assessment responsibilities; organizational personnel with security management responsibilities].
SG.CA-4	Smart Grid information system Connections	SG.CA-4.1 Determine if the organization authorizes all connections from the Smart Grid information system to other Smart Grid information systems.  SG.CA-4.2 Determine if the organization documents the Smart Grid information system connections and associated security requirements for each connection.  SG.CA-4.3 Determine if the organization monitors the Smart Grid information system connections on an ongoing basis, verifying enforcement of documented security requirements.	Examine, Interview	Examine: [SELECT FROM: Access control policy; procedures addressing Smart Grid information system connections; system and communications protection policy; Smart Grid information system interconnection security agreements; security plan; Smart Grid information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibility for developing, implementing, or approving Smart Grid information system interconnection agreements].
SG.CA-5	Security Authorization to Operate	SG.CA-5.1 Determine if 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.  SG.CA-5.2 Determine if: (i) the organization documents a management authority to sign and approve the security authorization to operate; (ii) the documented management authority signs and approves the security authorization to operate (iii) the organization needs to conduct security assessments in	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; risk management policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security authorization responsibilities for Smart Grid information systems; organizational personnel with risk management responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		support of security authorizations on an organization-defined frequency; (iv) the organization needs to review security assessments in support of security authorizations on an organization-defined frequency.		
SG.CA-6	Continuous Monitoring	SG.CA-6.1 Determine if: (i) the organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a) ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy; and b) reporting the security state of the Smart Grid information system to management authority on an organization-defined frequency; (ii) the organization documents the management authority receiving the security state reports of the Smart Grid information system; (iii) the organization defines the organizational frequency for reporting the security state of the Smart Grid information system to the management authority.	Examine, Interview, Test	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing continuous monitoring of Smart Grid information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; Smart Grid information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities].  Test: [SELECT FROM: Automated mechanisms implementing monitoring capability within the Smart Grid information system].
<b>Configuration Management (SG.CM)</b>				
SG.CM-1	Configuration Management Policy and Procedures	SG.CM-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) A documented configuration management security policy that addresses— 1) the objectives, roles, and responsibilities for the configuration management security program as it relates to protecting the organization’s personnel and assets; and 2) 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.  SG.CM-1.2 Determine if management commitment ensures compliance with the organization’s security policy and other regulatory requirements.  SG.CM-1.3 Determine if the organization ensures that the configuration	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		management security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.CM-2	Baseline Configuration	SG.CM-2.1 Determine if: (i) the organization a) develops the current baseline configuration of the Smart Grid information system; b) documents the current baseline configuration of the Smart Grid information system; c) maintains the current baseline configuration of the Smart Grid information system; d) implements the current baseline configuration of the Smart Grid information system; (ii) the organization maintains an inventory of the Smart Grid information system's constituent components; (iii) the organization reviews the baseline configuration as an integral part of Smart Grid information system component installations on an organizational defined frequency; (iv) the organization updates the baseline configuration as an integral part of Smart Grid information system component installations on an organizational defined frequency.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the Smart Grid information system; list of software authorized to execute on the Smart Grid information system; enterprise / Smart Grid information system architecture documentation; Smart Grid information system design documentation; Smart Grid information system architecture and configuration documentation; historical copies of baseline configurations; security plan; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with configuration change control responsibilities].
SG.CM-3	Configuration Change Control	SG.CM-3.1 Determine if: (i) the organization documents changes to the Smart Grid information system; (ii) the organization authorizes changes to the Smart Grid information system.  SG.CM-3.2 Determine if: (i) the organization retains records of configuration-managed changes to the Smart Grid information system; (ii) the organization reviews records of configuration-managed changes to the Smart Grid information system on an organizational defined frequency.  SG.CM-3.3 Determine if the organization audits activities associated with configuration-managed changes to the Smart Grid information system.  SG.CM-3.4 Determine if: (i) the organization tests configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing Smart Grid information system configuration change control; Smart Grid information system design documentation; Smart Grid information system architecture and configuration documentation; automated configuration control mechanisms; change control records; Smart Grid information system audit records; security plan; System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer / integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with configuration change control responsibilities; Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		information system; (ii) the organization validates configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system; (iii) the organization documents configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system.		
SG.CM-4	Monitoring Configuration Changes	SG.CM-4.1 Determine if: (i) the organization documents a process to monitor changes to the Smart Grid information system; (ii) the organization implements a process to monitor changes to the Smart Grid information system.  SG.CM-4.2 Determine if the organization, prior to change implementation and as part of the change approval process, analyzes changes to the Smart Grid information system for potential security impacts.  SG.CM-4.3 Determine if the organization, after the Smart Grid information system is changed, checks the security features to ensure that the features are still functioning properly.	Examine, Interview, Test	Examine: [SELECT FROM: configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the Smart Grid information system; security impact analysis documentation; Smart Grid information system architecture and configuration documentation; change control records; Smart Grid information system audit records; security plan; System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer / integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for determining security impacts prior to implementation of Smart Grid information system changes; Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].  Test: [SELECT FROM: Automated mechanisms implementing configuration change control].
SG.CM-5	Access Restrictions for Configuration Change	SG.CM-5.1 Determine if: (i) the organization defines individual access privileges associated with configuration changes to the Smart Grid information system; (ii) the organization documents individual access privileges associated with configuration changes to the Smart Grid information system; (iii) the organization approves individual access privileges associated with configuration changes to the Smart Grid information system; (iv) the organization enforces access restrictions associated with configuration changes to the Smart Grid information system.  SG.CM-5.2	Examine, Interview, Test	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the Smart Grid information system; list of critical software programs to be prohibited from installation without an approved certificate; Smart Grid information system design documentation; security plan; Smart Grid information system architecture and configuration documentation; change control records; Smart Grid information system audit records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; Organizational personnel responsible for enforcing a two-person rule for

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization generates records reflecting changes to individual access privileges on the Smart Grid information system;</li> <li>(ii) the organization retains records reflecting changes to individual access privileges on the Smart Grid information system;</li> <li>(iii) the organization reviews records reflecting changes to individual access privileges on the Smart Grid information system.</li> </ul> <p>SG.CM-5.3 Determine if the organization establishes terms and conditions for installing any hardware, firmware, or software on Smart Grid information system devices.</p> <p>SG.CM-5.4 Determine if the organization conducts audits of Smart Grid information system changes at an organization-defined frequency and if/when suspected unauthorized changes have occurred.</p>		<p>system changes].</p> <p>Test: [SELECT FROM: Change control process and associated restrictions for changes to the Smart Grid information system; Automated mechanisms implementing access restrictions for changes to the Smart Grid information system; Smart Grid information system mechanisms preventing installation of software programs not signed with an organization-approved certificate; Smart Grid information system implementing safeguards and countermeasures for inappropriate changes to security functions].</p>
SG.CM-6	Configuration Settings	<p>SG.CM-6.1 Determine if the organization establishes configuration settings for components within the Smart Grid information system.</p> <p>SG.CM-6.2 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization monitors changes to the configuration settings in accordance with organizational policies and procedures;</li> <li>(ii) the organization controls changes to the configuration settings in accordance with organizational policies and procedures.</li> </ul> <p>SG.CM-6.3 Determine if the organization documents changed configuration settings.</p> <p>SG.CM-6.4 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization identifies exceptions from the configuration settings;</li> <li>(ii) the organization documents exceptions from the configuration settings;</li> <li>(iii) the organization approves exceptions from the configuration settings.</li> </ul> <p>SG.CM-6.5 Determine if the organization enforces the configuration settings in all components of the Smart Grid information system.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing configuration settings for the Smart Grid information system; security plan; incident response plan; Smart Grid information system design documentation Smart Grid information system configuration settings and associated documentation; security configuration checklists; Smart Grid information system design documentation; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing the centralized management, application, and verification of configuration settings; Automated mechanisms implementing responses to unauthorized changes to configuration settings].</p>
SG.CM-7	Configuration for Least Functionality	SG.CM-7.1 Determine if the organization configures the Smart Grid	Examine, Interview,	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing least

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>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.</p> <p>SG.CM-7.2 Determine if the organization 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.</p>	Test	<p>functionality in the Smart Grid information system; security plan; Smart Grid information system design documentation; specification of preventing software program execution; Smart Grid information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the Smart Grid information system].</p> <p>Test: [SELECT FROM: Smart Grid information system for disabling or restricting functions, ports, protocols, and services; Automated mechanisms preventing software program execution on the Smart Grid information system].</p>
SG.CM-8	Component Inventory	<p>SG.CM-8.1 Determine if the organization develops, documents, and maintains an inventory of the components of the Smart Grid information system that—</p> <ul style="list-style-type: none"> <li>a) accurately reflects the current Smart Grid information system configuration;</li> <li>b) provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability;</li> <li>c) identifies the roles responsible for component inventory;</li> <li>d) updates the inventory of system components as an integral part of component installations, system updates, and removals;</li> <li>e) ensures that the location (logical and physical) of each component is included within the Smart Grid information system boundary.</li> </ul>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Configuration management policy; configuration management plan; ; Smart Grid information system design documentation; Smart Grid information system inventory records procedures addressing Smart Grid information system component inventory; security plan; Smart Grid information system inventory records; Smart Grid information system inventory records; component installation records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system inventory responsibilities; organizational personnel with responsibilities for defining Smart Grid information system components within the authorization boundary of the system; Organizational personnel with Smart Grid information system installation and inventory responsibilities].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing Smart Grid information system component inventory management; Automated mechanisms for detecting unauthorized components/devices on the Smart Grid information system].</p>
SG.CM-9	Addition, Removal, and Disposal of Equipment	<p>SG.CM-9.1 Determine if the organization implements policy and procedures to address the addition, removal, and disposal of all Smart Grid information system equipment.</p> <p>SG.CM-9.1 Determine if all Smart Grid information system components and information are documented, identified, and tracked so that their</p>	Examine, Interview	<p>Examine: [SELECT FROM: Smart Grid information system media protection policy; media sanitization equipment test records; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media sanitization</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CM-10	Factory Default Settings Management	location and function are known. SG.CM-10.1 Determine if 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. SG.CM-10.2 Determine if: (i) the factory default settings are changed upon installation; (ii) the factory default settings are change used during maintenance.	Examine, Interview, Test	responsibilities]. Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing responsibilities for configuration management process development; configuration standard documents; procedures addressing configuration management planning; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for configuration management process development]. Test: [SELECT FROM: Automated mechanisms implementing standardize configurations].
SG.CM-11	Configuration Management Plan	SG.CM-11.1 Determine if the organization develops and implements a configuration management plan for the Smart Grid information system that— a) addresses roles, responsibilities, and configuration management processes and procedures; b) defines the configuration items for the Smart Grid information system; c) defines when (in the system development life cycle) the configuration items are placed under configuration management; d) defines the means for uniquely identifying configuration items throughout the system development life cycle; e) defines the process for managing the configuration of the controlled items.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing responsibilities for configuration management process development; procedures addressing configuration management planning; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for configuration management process development].
<b>Continuity of Operations (SG.CP)</b>				
SG.CP-1	Continuity of Operations Policy and Procedures	SG.CP-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) a documented continuity of operations security policy that addresses— 1) the objectives, roles, and responsibilities for the continuity of operations security program as it relates to protecting the organization’s personnel and assets; and 2) 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. SG.CP-1.2 Determine if:	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements.  SG.CP-1.3 Determine if the organization ensures that the continuity of operations security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.CP-2	Continuity of Operations Plan	SG.CP-2.1 Determine if: (i) the organization develops 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; (ii) the organization documents 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; (iii) the organization 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.  SG.CP-2.2 Determine if the organizational continuity of operations plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring Smart Grid information system operations after a disruption or failure.  SG.CP-2.3 Determine if: (i) the organization document a management authority for the continuity of operations plan; (ii) the management authority reviews and approves the continuity of operations plan.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy and procedures; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with contingency planning responsibilities].
SG.CP-3	Continuity of Operations Roles and Responsibilities	SG.CP-3.1 Determine if the organizational continuity of operations plan for Smart Grid information systems a) defines the roles and responsibilities of the various employees and contractors in the event of a significant incident; and b) identifies responsible personnel to lead the recovery and response effort if an incident occurs.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the Smart Grid information system; contingency plan; security plan; business impact assessment; other related plans; alternate processing site agreements; alternate storage site agreements; contingency plan testing and / or exercise documentation; contingency plan test results; other relevant documents or records].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas; organizational personnel with incident handling responsibilities].
SG.CP-4	Continuity of Operations Training	SG.CP-4.1 Determine if: (i) the organization trains personnel in their continuity of operations roles and responsibilities with respect to the Smart Grid information system; (ii) the organization provides refresher training on their continuity of operations roles and responsibility with respect to the Smart Grid information system on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with contingency planning, plan implementation, and training responsibilities].
SG.CP-5	Continuity of Operations Plan Testing	SG.CP-5.1 Determine if: (i) the continuity of operations plan is tested to determine its effectiveness; (ii) the continuity of operations plan testing results are documents.  SG.CP-5.2 Determine if: (i) the organization documented a management authority to review continuity of operations plan test results (ii) the management authority reviews the documented test results and initiates corrective actions, if necessary.  SG.CP-5.3 Determine if the organization tests the continuity of operations plan for the Smart Grid information system on an organization-defined frequency, using defined tests.  SG.CP-5.4 (requirement enhancements 1) Determine if the organization coordinates continuity of operations plan testing and exercises with all affected organizational elements.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; automated mechanisms supporting contingency plan testing/exercises; contingency plan testing and / or exercise documentation; contingency plan test results; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises; Organizational personnel with Smart Grid information system recovery and reconstitution responsibilities; organizational personnel with contingency plan testing and / or exercise responsibilities; Organizational personnel with contingency planning, plan implementation, and testing responsibilities; organizational personnel with responsibilities for related plans].
SG.CP-6	Continuity of Operations Plan Update	SG.CP-6.1 Determine if: (i) the organization reviews the continuity of operations plan for the Smart Grid information system on an organizational defined frequency; (ii) the organization updates the continuity of operations 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.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the Smart Grid information system; contingency plan; security plan; business impact assessment; other related plans; alternate processing site agreements; alternate storage site agreements; contingency plan testing and / or exercise documentation; contingency plan test results; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas; organizational

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CP-7	Alternate Storage Sites	<p>SG.CP-7.1 Determine if: (i) the organization determines the requirement for an alternate storage site for continuity of operations; (ii) the organization initiates any necessary agreements for an alternate storage site for continuity of operations.</p> <p>SG.CP-7.2 (requirement enhancements 1) Determine if 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.</p> <p>SG.CP-7.3 (requirement enhancements 2) Determine if 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.</p> <p>SG.CP-7.4 (requirement enhancements 3) Determine if the organization configures the alternate storage site to facilitate timely and effective recovery operations.</p>	Examine, Interview	<p>personnel with incident handling responsibilities].</p> <p>Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; alternate storage site agreements; mitigation actions for accessibility problems to the alternate storage site; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas; organizational personnel with incident handling responsibilities].</p>
SG.CP-8	Alternate Telecommunication Services	<p>SG.CP-8.1 Determine if: (i) the organization identifies alternate telecommunication services for the Smart Grid information system for continuity of operations; (ii) the organization 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.</p> <p>SG.CP-8.2 (requirement enhancement 1) Determine if: (i) primary telecommunication service agreements contain priority-of-service provisions in accordance with the organization's availability requirements; (ii) alternate telecommunication service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.</p> <p>SG.CP-8.3 (requirement enhancement 2) Determine if alternate telecommunication services do not share a single point of failure with primary telecommunication services.</p> <p>SG.CP-8.4 (requirement enhancement 3) Determine if alternate telecommunication service providers need to</p>	Examine, Interview	<p>Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; list of essential missions and business functions; primary telecommunications service provider's site; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		be sufficiently separated from primary service providers so they are not susceptible to the same hazards.  SG.CP-8.5 (requirement enhancement 4) Determine if (i) primary telecommunication service providers need to have adequate contingency plans; (ii) alternate telecommunication service providers need to have adequate contingency plans.		
SG.CP-9	Alternate Control Center	SG.CP-9.1 Determine if the organization identifies an alternate control center 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 that includes a) necessary telecommunications b) initiates any necessary agreements.  SG.CP-9.2 (requirement enhancements 1) Determine if 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 for continuity of operations.  SG.CP-9.3 (requirement enhancements 2) Determine if 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.  SG.CP-9.4 (requirement enhancements 3) Determine if the organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; list of essential missions and business functions; primary telecommunications service provider's site; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers].
SG.CP-10	Smart Grid information system Recovery and Reconstitution	SG.CP-10.1 Determine if: (i) 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; (ii) the organization documents the Smart Grid information system secure state.  SG.CP-10.2 (requirement enhancement 1) Determine if the organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state.	Examine, Interview, Test	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing Smart Grid information system recovery and reconstitution; Smart Grid information system configuration settings and associated documentation; Smart Grid information system design documentation; Smart Grid information system design documentation; contingency plan test results; location(s) of backup and restoration hardware, firmware, and software; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system recovery and reconstitution responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.CP-10.3 (requirement enhancement 2) Determine if 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.		Test: [SELECT FROM: Automated mechanisms and / or manual procedures for implementing Smart Grid information system recovery and reconstitution operations; Failover capability for the Smart Grid information system].
SG.CP-11	Fail-Safe Response	SG.CP-11.1 Determine if 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.	Examine, Interview, Test	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing Smart Grid information system recovery and reconstitution; Smart Grid information system configuration settings and associated documentation; Smart Grid information system design documentation; Smart Grid information system design documentation; contingency plan test results; location(s) of backup and restoration hardware, firmware, and software; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system recovery and reconstitution responsibilities].  Test: [SELECT FROM: Automated mechanisms and / or manual procedures for implementing Smart Grid information system recovery and reconstitution operations; Failover capability for the Smart Grid information system].
<b>Identification and Authentication (SG.IA)</b>				
SG.IA-1	Identification and Authentication Policy and Procedures	SG.IA-1.1 Determine if: (i) the organization develops and implements a documented identification and authentication policy; (ii) the identification and authentication policy addresses identification and authentication as it related to protecting the organization's personnel and assets and the following: a) purpose / objective b) scope c) roles and responsibilities d) coordination among organizational entities, and compliance; (iii) the identification and authentication policy addresses the scope to include all organizational staff, contractors, and third parties; (iv) the organization develops and implements the identification and authentication procedures; (v) the organization reviews and updates the identification and authentication procedures (COVERED in SG.IA.2(i)); (vi) management commitment ensures compliance with the organization's identification and authentication policy, security policy and other regulatory requirements;	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>(vii) the identification and authentication policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and</p> <p>(viii) the identification and authentication procedures facilitate implementation of the identification and authentication security policy.</p> <p>SG.IA-1.2 Determine if:</p> <p>(i) the organization defines the frequency of identification and authentication policy and procedures reviews/updates;</p> <p>(ii) the organization reviews/updates the identification and authentication policy and procedures in accordance with the organization-defined frequency.</p>		
SG.IA-2	Identifier Management	<p>SG.IA-2.1 Determine if the organization received authorization from a management authority to assign a user or device identifier.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of Smart Grid information system accounts; list of characteristics identifying user status; list of identifiers generated from physical access control devices; identifier certification documentation; organizational personnel biometrics records; procedures addressing account management; user ID and password registration documentation; ID and password authorization records; registration authority records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with identifier management responsibilities].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing identifier management functions].</p>
SG.IA-3	Authenticator Management	<p>SG-IA-3.1 Determine if the organization manages the Smart Grid information system authentication credential for users and devices by</p> <p>(a) defining initial authentication credential content, such as defining password length and composition, tokens;</p> <p>(b) establishing administrative procedures for</p> <ol style="list-style-type: none"> <li>1) initial authentication credential distribution</li> <li>2) lost, compromised, or damaged authentication credentials</li> <li>3) revoking authentication credentials;</li> </ol> <p>(c) Changing/refreshing authentication credentials on an organization-defined frequency; and</p> <p>(d) Specifying measures to safeguard authentication credentials.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; Smart Grid information system design documentation; system and services acquisition policy; procedures addressing authenticator management; procedures addressing the integration of security requirements into the acquisition process; acquisition documentation; acquisition contracts for Smart Grid information system procurements or services; Smart Grid information system configuration settings and associated documentation; logical access scripts; automated tools for</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG-IA-3.2 Determine if the organization defines the frequency for authentication credential changing / refreshing.		testing authenticators; application code reviews for detecting unencrypted static authenticators; security plan; list of individuals having accounts on multiple Smart Grid information systems; information classification or sensitivity documentation; security categorization documentation for the Smart Grid information system; security assessments of authenticator protections; risk assessment results; list of measures intended to manage risk of compromise due to individuals having accounts on multiple Smart Grid information systems; PKI certification revocation lists; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for determining initial authenticator content; Organizational personnel with authenticator management responsibilities; organizational personnel implementing and / or maintaining authenticator protections; Organizational personnel with responsibilities for PKI-based authentication management; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].  Test: [SELECT FROM: Automated mechanisms implementing authenticator management functions; Automated mechanisms implementing PKI-based authenticator management functions; Automated mechanisms for authenticator strength].
SG-IA-4	User Identification and Authentication	SG-IA-4.1 Determine if: (i) the organization uniquely identifies users; (ii) the organization authenticates users.	Examine, Interview, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; list of Smart Grid information system accounts; list of privileged Smart Grid information system accounts; list of non-privileged Smart Grid information system accounts; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for determining initial authenticator content; Organizational personnel with authenticator management responsibilities; organizational personnel implementing and / or maintaining authenticator protections; Organizational personnel with responsibilities for PKI-based authentication management; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Test: [SELECT FROM: Automated mechanisms implementing identification and authentication capability for the Smart Grid information system].
SG.IA-5	Device Identification and Authentication	<p>SG.IA-5.1 Determine if: (i) the organization uniquely identified an organization-defined list of devices before establishing a connection; (ii) the organization authenticates an organization-defined list of devices before establishing a connection.</p> <p>SG.IA-5.1 Determine if: (i) The Smart Grid information system authenticates devices before establishing remote network connections using bidirectional authentication between devices that is cryptographically based; (ii) the Smart Grid information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Identification and authentication policy; procedures addressing device identification and authentication; Smart Grid information system design documentation; list of devices requiring unique identification and authentication; device connection reports; Smart Grid information system configuration settings and associated documentation; DHCP lease information; device connection reports; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with responsibilities for determining initial authenticator content; Organizational personnel with authenticator management responsibilities; organizational personnel implementing and / or maintaining authenticator protections; Organizational personnel with responsibilities for PKI-based authentication management; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing device identification and authentication].</p>
SG.IA-6	Authenticator Feedback	SG.IA-6.1 Determine if the organization 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.	Examine, Test	<p>Examine: [SELECT FROM: Identification and authentication policy; procedures addressing authenticator feedback; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing authenticator feedback].</p>
<b>Information and Document Management (SG.ID)</b>				
SG.ID-1	Information and Document Management Policy and Procedures	<p>SG.ID-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) a Smart Grid information and document management policy that addresses— 1) the objectives, roles and responsibilities for the information and document management security program as it relates to protecting the organization’s personnel and assets; 2) the scope of the information and document management security program as it applies to all the organizational staff, contractors, and third parties; 3) the retrieval of written and electronic records, equipment,</p>	Examine, Interview	<p>Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>and other media for the Smart Grid information system; and</p> <p>4) the destruction of written and electronic records, equipment, and other media for the Smart Grid information system; and</p> <p>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.</p> <p>SG.ID-1.2 Determine if management commitment ensures compliance of the organization's security policy and other regulatory requirements.</p> <p>SG.ID-1.3 Determine if 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.</p>		
SG.ID-2	Information and Document Retention	<p>SG.ID-2.1 Determine if the organization develops policies and procedures detailing the retention of organization information.</p> <p>SG.ID-2.2 Determine if the organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations.</p> <p>SG.ID-2.3 Determine if the organization manages Smart Grid information system-related data including establishing retention policies and procedures for both electronic and paper data.</p> <p>SG.ID-2.4 Determine if the organization manages access to Smart Grid information system-related data based on assigned roles and responsibilities.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; Smart Grid information system audit records System and information integrity policy; procedures addressing Smart Grid information system output handling and retention; media protection policy and procedures; information retention records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record retention responsibilities; Organizational personnel with information output handling and retention responsibilities].</p>
SG.ID-3	Information Handling	<p>SG.ID-3.1 Determine if:</p> <p>(i) the organization-implemented policies and procedures detailing the handling of information are developed;</p> <p>(ii) the organization-implemented policies and procedures detailing the handling of information are reviewed on an organization-defined frequency.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Media protection policy and procedures; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection responsibilities].</p>
SG.ID-4	Information Exchange	<p>SG.ID-4.1 Determine if organizational agreements are established for the exchange of information, firmware, and software between the</p>	Examine, Interview	<p>Examine: [SELECT FROM: Security planning policy; access control policy; contingency planning policy; security plan for the Smart Grid information system; contingency plan for the</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		organization and external parties such as third parties, vendors and contractors.		<p>Smart Grid information system; Smart Grid information system design documentation; boundary protection procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; procedures addressing the use of external Smart Grid information systems; security plan; Smart Grid information system connection or processing agreements; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organization personnel with security planning and plan implementation responsibilities for the Smart Grid information system; Organizational personnel with responsibility for developing, implementing, or approving Smart Grid information system interconnection agreements].</p>
SG.ID-5	Automated Labeling	<p>SG.ID-5.1 Determine if the Smart Grid information system automatically labels information in storage, in process, and in transmission in accordance with—</p> <ul style="list-style-type: none"> <li>a) access control requirements;</li> <li>b) special dissemination, handling, or distribution instructions;</li> </ul> <p>and</p> <ul style="list-style-type: none"> <li>c) otherwise as required by the Smart Grid information system security policy.</li> </ul>	Examine, Interview	<p>Examine: [SELECT FROM: Smart Grid information system marking protection policy; procedures addressing information labeling; security plan; storage media and Smart Grid information system output; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system information protection and marking responsibilities].</p>
<b>Incident Response (SG.IR)</b>				
SG.IR-1	Incident Response Policy and Procedures	<p>SG.IR-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency—</p> <ul style="list-style-type: none"> <li>a) a documented incident response security policy that addresses—                             <ul style="list-style-type: none"> <li>1) the objectives, roles, and responsibilities for the incident response security program as it relates to protecting the organization's personnel and assets; and</li> <li>2) the scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties; and</li> </ul> </li> <li>b) procedures to address the implementation of the incident response security policy and associated incident response protection requirements.</li> </ul> <p>SG.IR-1.2 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents management's commitment to ensure compliance with the organization's security policy and other regulatory requirements;</li> <li>(ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements.</li> </ul>	Examine, Interview	<p>Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.IR-1.3 Determine if the organization ensures that the incident response security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.  SG.IR-1.4 Determine if the organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood."		
SG.IR-2	Incident Response Roles and Responsibilities	SG.IR-2.1 Determine if the organization's Smart Grid information system security plan defines the specific roles and responsibilities in relation to various types of incidents.  SG.IR-2.2 Determine if: (i) the plan identifies responsible personnel to lead the response effort if an incident occurs; (ii) the organization forms documents response teams to include Smart Grid information system and other process owners, to reestablish operations.	Examine, Interview	Examine: [SELECT FROM: Incident response policy and procedures; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with incident response responsibilities].
SG.IR-3	Incident Response Training	SG.IR-3.1 Determine if: (i) personnel are trained in their incident response roles and responsibilities with respect to the Smart Grid information system on an organization-defined frequency; (ii) personnel refresher training on an organization-defined frequency for their incident response roles and responsibilities with respect to the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident response training; automated mechanisms supporting incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with incident response training and operational responsibilities].
SG.IR-4	Incident Response Testing and Exercises	SG.IR-4.1 Determine if: (i) the organization tests and / or exercises the incident response capability for the Smart Grid information system at an organization-defined frequency using organization-defined tests and / or exercises to determine the incident response effectiveness and documents the results; (ii) the organization documents the test and / or exercise results on the incident response capability for the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing documentation; automated mechanisms supporting incident response tests/exercises; incident response plan; incident response testing material; incident response test results; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with incident response testing responsibilities].
SG.IR-5	Incident Handling	SG.IR-5.1 Determine if: (i) the organization implements an incident handling capability for security incidents that includes a) preparation b) detection	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident handling; incident response plan; automated mechanisms supporting incident handling; security plan; incident response plan; other relevant documents or records].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		c) analysis d) containment e) mitigation f) recovery; (ii) the organization integrates incident handling procedures with continuity of operations procedures; (iii) the organization incorporates lessons learned from incident handling activities into incident response procedures.		Interview: [SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities].  Test: [SELECT FROM: Incident handling capability for the organization].
SG.IR-6	Incident Monitoring	SG.IR-6.1 Determine if: (i) the organization tracks Smart Grid information system and network security incidents; (ii) the organization documents Smart Grid information system and network security incidents.	Examine, Interview, Test	Examine: [SELECT FROM: Incident response policy; procedures addressing incident monitoring; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; incident response records and documentation; automated mechanisms supporting incident monitoring; incident response plan; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with incident monitoring responsibilities].  Test: [SELECT FROM: Incident monitoring capability for the organization; Automated mechanisms assisting in tracking of security incidents and in the collection and analysis of incident information].
SG.IR-7	Incident Reporting	SG.IR-7.1 Determine if 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.  SG.IR-7.2 Determine if the organization's detailed incident data is reported in a manner that complies with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; automated mechanisms supporting incident reporting; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with incident reporting responsibilities].
SG.IR-8	Incident Response Investigation and Analysis	SG.IR-8.1 Determine if the organization policies and procedures include an incident response investigation and analysis program.  SG.IR-8.2 Determine if the organization includes investigation and analysis of Smart Grid information system incidents in the planning process.  SG.IR-8.3 Determine if: (i) the organization develops an incident investigation and analysis	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm / surveillance equipment logs or records; Smart Grid information system design documentation; security plan; physical access logs or records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with physical access monitoring responsibilities].  Test: [SELECT FROM: Physical access monitoring capability;

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		process; (ii) the organization tests an incident investigation and analysis process; (iii) the organization deploys an incident investigation and analysis process; (iv) the organization documents an incident investigation and analysis process.		Automated mechanisms implementing physical access monitoring capability].
SG.IR-9	Corrective Action	SG.IR-9.1 Determine if the organization reviews investigation results and determines corrective actions needed.  SG.IR-9.2 Determine if the organization 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.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm / surveillance equipment logs or records; Smart Grid information system design documentation; security plan; physical access logs or records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with physical access monitoring responsibilities].
SG.IR-10	Smart Grid information system Backup	SG.IR-10.1 Determine if the organization conducts backups of user-level information contained in the Smart Grid information system on an organization-defined frequency.  SG.IR-10.2 Determine if the organization 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.  SG.IR-10.3 Determine if the organization conducts backups of Smart Grid information system documentation including security-related documentation on an organization-defined frequency consistent with recovery time.  SG.IR-10.4 Determine if the organization protects the confidentiality and integrity of backup information at the storage location.  SG.IR-10.5 (requirement enhancements 1) Determine if the organization tests backup information at an organization-defined frequency to verify media reliability and information integrity.  SG.IR-10.6 (requirement enhancements 2) Determine if the organization selectively uses backup information in the restoration of Smart Grid information system functions as part of continuity of operations testing.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing Smart Grid information system backup; Smart Grid information system backup test results; contingency plan test results; contingency plan testing and / or exercise documentation; backup storage location(s); secondary backup storage location(s); redundant secondary system for Smart Grid information system backups; security plan alternate site service agreements; backup storage location(s); Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with Smart Grid information system backup responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.IR-10.7 (requirement enhancements 3) Determine if 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.		
SG.IR-11	Coordination of Emergency Response	SG.IR-10.1 Determine if: (i) the organization's security policies and procedures delineate how the organization implements its emergency response plan; (ii) the organization's security policies and procedures coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.	Examine, Interview	Examine: [SELECT FROM: Incident response / emergency management policy; procedures addressing incident response planning; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities].
<b>Smart Grid information system Development and Maintenance (SG.MA)</b>				
SG.MA-1	Smart Grid information system Maintenance Policy and Procedures	SG.MA-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) A documented Smart Grid information system maintenance security policy that addresses— 1) 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 2) 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.  SG.MA-1.2 Determine if: (i) the organization documents management's commitment to ensure compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements.  SG.MA-1.3 Determine if 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.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.MA-2	Legacy Smart Grid information system	SG.MA-2.1 Determine if the organization develops policies and procedures to	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing security-related activity planning for the Smart Grid

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
	Updates	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.		<p>information system; Smart Grid information system maintenance policy; procedures addressing controlled maintenance for the Smart Grid information system; maintenance records; manufacturer / vendor maintenance specifications; equipment sanitization records; media sanitization records; automated mechanisms supporting Smart Grid information system maintenance activities; Smart Grid information system configuration settings and associated documentation; maintenance records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities; Organizational personnel with Smart Grid information system maintenance responsibilities].</p>
SG.MA-3	Smart Grid information system Maintenance	<p>SG.MA-3.1 Determine if: (i) the organization schedules maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; (ii) the organization performs maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; (iii) the organization documents maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; (iv) the organization reviews records of maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements.</p> <p>SG.MA-3.2 Determine if the organization 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.</p> <p>SG.MA-3.3 Determine if the organization sanitizes the equipment to remove all critical/sensitive information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Security planning policy; procedures addressing security-related activity planning for the Smart Grid information system; Smart Grid information system maintenance policy; procedures addressing controlled maintenance for the Smart Grid information system; maintenance records; manufacturer / vendor maintenance specifications; equipment sanitization records; media sanitization records; automated mechanisms supporting Smart Grid information system maintenance activities; Smart Grid information system configuration settings and associated documentation; maintenance records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities; Organizational personnel with Smart Grid information system maintenance responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>SG.MA-3.4 Determine if the organization checks all potentially impacted security requirements to verify that the requirements are still functioning properly following maintenance or repair actions.</p> <p>SG.MA-3.5 Determine if the organization makes and secures backups of critical Smart Grid information system software, applications, and data for use if the operating system becomes corrupted or destroyed.</p> <p>SG.MA-3.6 (requirement enhancement 1) Determine if 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).</p>		
SG.MA-4	Maintenance Tools	<p>SG.MA-4.1 Determine if:                      (i) the organization approves the use of Smart Grid information system maintenance tools;                      (ii) the organization monitors the use of Smart Grid information system maintenance tools.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Smart Grid information system maintenance policy; Smart Grid information system maintenance tools and associated documentation; procedures addressing Smart Grid information system maintenance tools; automated mechanisms supporting Smart Grid information system maintenance activities; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; maintenance records; Smart Grid information system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities].</p> <p>Test: [SELECT FROM: Automated mechanisms supporting Smart Grid information system maintenance activities; Media checking process for malicious code detection].</p>
SG.MA-5	Maintenance Personnel	<p>SG.MA-5.1 Determine if 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.</p> <p>SG.MA-5.2</p>	Examine, Interview	<p>Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing maintenance personnel; Smart Grid information system media protection policy; physical and environmental protection policy; security plan; list of maintenance personnel requiring escort / supervision; maintenance records; access control policy and procedures; physical and environmental protection policy and</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>Determine if authorized organizational personnel with appropriate maintenance access supervise unauthorized maintenance personnel during the performance of maintenance activities on the Smart Grid information system.</p>		<p>procedures; memorandum of agreement; maintenance records; access control records; service provider contracts and / or service level agreements; list of authorized personnel; maintenance records; maintenance records; access authorizations; access credentials; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities].</p>
SG.MA-6	Remote Maintenance	<p>SG.MA-6.1 Determine if the organization policy and procedures for remote maintenance include:                      a) authorization and monitoring the use of remote maintenance and diagnostic activities;                      b) use of remote maintenance and diagnostic tools;                      c) maintenance records for remote maintenance and diagnostic activities;                      d) termination of all remote maintenance sessions; and                      e) management of authorization credentials used during remote maintenance.</p> <p>SG.MA-6.2 (requirement enhancement 1) Determine if the organization requires that remote maintenance or diagnostic services be performed from a Smart Grid information system that implements a level of security at least as high as that implemented on the Smart Grid information system being serviced.</p> <p>SG.MA-6.3 (requirement enhancement 2) Determine if 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.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing non-local maintenance for the Smart Grid information system; service provider contracts and / or service level agreements; cryptographic mechanisms supporting Smart Grid information system maintenance activities; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; maintenance records; security plan; audit records; maintenance records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities; Smart Grid information system maintenance provider].</p>
SG.MA-7	Timely Maintenance	<p>SG.MA-7.1 Determine if:                      (i) the organization obtains maintenance support for an organization-defined list of security-critical Smart Grid information system components;                      (ii) the organization obtains spare parts for an organization-defined list of security-critical Smart Grid information system components.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing timely maintenance for the Smart Grid information system; service provider contracts and / or service level agreements; inventory and availability of spare parts; security plan; other relevant documents or records].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
<b>Media Protection (SG.MP)</b>				
SG.MP-1	Media Protection Policy and Procedures	<p>SG.MP-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency—</p> <ul style="list-style-type: none"> <li>a) A documented media protection security policy that addresses—                             <ul style="list-style-type: none"> <li>1) The objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization’s personnel and assets; and</li> <li>2) The scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and</li> </ul> </li> <li>b) Procedures to address the implementation of the media protection security policy and associated media protection requirements.</li> </ul> <p>SG.MP-1.2 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents management commitment to ensure compliance with the organization’s security policy and other regulatory requirement;</li> <li>(ii) management commitment ensures compliance with the organization’s security policy and other regulatory requirements.</li> </ul> <p>SG.MP-1.3 Determine if the organization ensures that the media protection security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>
SG.MP-2	Media Sensitivity Level	<p>SG.MP-2.1 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents the sensitivity levels of media;</li> <li>(ii) the sensitivity level of media indicates the protection required commensurate with the impact of compromise.</li> </ul>	Examine, Interview	<p>Examine: [SELECT FROM: Risk assessment policy; procedures addressing security categorization of organizational information and Smart Grid information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities].</p>
SG.MP-3	Media Marking	<p>SG.MP-3.1 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization marks removable Smart Grid information system media in accordance with organization-defined policy and procedures;</li> <li>(ii) the organization marks Smart Grid information system output in accordance with organization-defined policy and procedures.</li> </ul>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and Smart Grid information system output; other relevant documents or records].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				<p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection and marking responsibilities].</p> <p>Test: [SELECT FROM: Automated mechanisms supporting removable media marking; Media checking process for markings on removable media; Removable media].</p>
SG.MP-4	Media Storage	<p>SG.MP-4.1 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents the storage requirements of stored media;</li> <li>(ii) the organization physically manages Smart Grid information system media within protected areas;</li> <li>(iii) the organization physically stores Smart Grid information system media within protected areas.</li> </ul>	Examine, Interview	<p>Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; security plan; Smart Grid information system media; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection and storage responsibilities].</p>
SG.MP-5	Media Transport	<p>SG.MP-5.1 Determine if the organization protects organization-defined types of media during transport outside controlled areas using organization-defined security measures.</p> <p>SG.MP-5.2 Determine if the organization maintains accountability for Smart Grid information system media during transport outside controlled areas.</p> <p>SG.MP-5.3 Determine if the organization restricts the activities associated with transport of such media to authorized personnel.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; list of organization-defined personnel authorized to transport Smart Grid information system media outside of controlled areas; Smart Grid information system media; Smart Grid information system media transport records; Smart Grid information system audit records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media transport responsibilities].</p> <p>Test: [SELECT FROM: Mechanisms protecting information during transportation outside controlled areas].</p>
SG.MP-6	Media Sanitization and Disposal	<p>SG.MP-6.1 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization sanitizes Smart Grid information system media before disposal or release for reuse;</li> <li>(ii) the organization tests sanitization equipment and procedures to verify correct performance on an organization-defined frequency.</li> </ul> <p>SG.MP-6.2 (requirement enhancement 1) Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization tracks media sanitization and disposal actions;</li> </ul>	Examine, Interview	<p>Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; media sanitization equipment test records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media sanitization responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(ii) the organization documents media sanitization and disposal actions; (iii) the organization verifies media sanitization and disposal actions.		
<b>Physical and Environmental Security (SG.PE)</b>				
SG.PE-1	Physical and Environmental Security Policy and Procedures	<p>SG.PE-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency—</p> <ul style="list-style-type: none"> <li>a) A documented physical and environmental security policy that addresses—                             <ul style="list-style-type: none"> <li>1) The objectives, roles, and responsibilities for the physical and environmental security program as it relates to protecting the organization’s personnel and assets; and</li> <li>2) The scope of the physical and environmental security program as it applies to all of the organizational staff, contractors, and third parties; and</li> </ul> </li> <li>b) Procedures to address the implementation of the physical and environmental security policy and associated physical and environmental protection requirements.</li> </ul> <p>SG.PE-1.2 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents management commitment to ensure compliance with the organization’s security policy and other regulatory requirement;</li> <li>(ii) management commitment ensures compliance with the organization’s security policy and other regulatory requirements.</li> </ul> <p>SG.PE-1.3 Determine if the organization ensures that the physical and environmental security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>
SG.PE-2	Physical Access Authorizations	<p>SG.PE-2.1 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization develops lists of personnel with authorized access to facilities containing Smart Grid information systems;</li> <li>(ii) the organization maintains lists of personnel with authorized access to facilities containing Smart Grid information systems;</li> <li>(iii) the organization issues appropriate authorization credential to personnel for facilities containing Smart Grid information systems.</li> </ul> <p>SG.PE-2.2 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents designated officials to review and approval access lists for authorization credential to personnel for</li> </ul>	Examine, Interview	<p>Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; physical access control logs or records; Smart Grid information system entry and exit points; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to Smart Grid information system facility].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		facilities containing Smart Grid information systems; (ii) designated officials within the organization review, update and approve access lists on an organization-defined frequency.		
SG.PE-3	Physical Access	<p>SG.PE-3.1 Determine if: (i) the organization documents all physical access authorizations for all physical access points to the facility where the Smart Grid information system resides; (ii) the organization enforces physical access authorizations for all physical access points to the facility where the Smart Grid information system resides.</p> <p>SG.PE-3.2 Determine if the organization verifies individual access authorizations before granting access to the facility.</p> <p>SG.PE-3.3 Determine if the organization controls entry to facilities containing Smart Grid information systems.</p> <p>SG.PE-3.4 Determine if the organization secures keys, combinations, and other physical access devices.</p> <p>SG.PE-3.5 Determine if the organization inventories physical access devices on a periodic basis.</p> <p>SG.PE-3.6 Determine if: (i) the organization changes combinations, keys, and authorization credentials on an organization-defined frequency; (ii) the organization changes combinations, keys, and authorization credentials when a) keys are lost b) combinations are compromised c) individual credentials are lost d) individuals are transferred e) individuals are terminated.</p> <p>SG.PE-3.7 (requirement enhancement 1) Determine if the organization requires physical access mechanisms to Smart Grid information system assets in addition to physical access mechanisms to the facility.</p> <p>SG.PE-3.8 (requirement enhancement 2)</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing access control for display medium; facility surveillance records; records of security checks; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; facility layout documentation; Smart Grid information system entry and exit points; list of Smart Grid information system components requiring protection through lockable physical casings; lockable physical casings; facility layout of Smart Grid information system components; actual displays from Smart Grid information system components; Smart Grid information system design documentation; facility communications and wiring diagrams; procedures addressing physical access control; physical access control logs or records; procedures addressing penetration testing; rules of engagement and associated documentation; penetration test results; security plan; list of areas within the facility containing high concentrations of Smart Grid information system components or Smart Grid information system components requiring additional physical protection; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with physical access control responsibilities].</p> <p>Test: [SELECT FROM: Physical access control capability; physical access control devices].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if the organization employs hardware to deter unauthorized physical access to Smart Grid information system devices.		
SG.PE-4	Monitoring Physical Access	<p>SG.PE-4.1 Determine if the organization monitors physical access to the Smart Grid information system to detect and respond to physical security incidents.</p> <p>SG.PE-4.2 Determine if: (i) the organization logs physical access to the Smart Grid information system; (ii) the organization reviews physical access logs on an organization-defined frequency.</p> <p>SG.PE-4.3 Determine if: (i) the organization coordinates results of reviews with the organization's incident response capability; (ii) the organization coordinates results of investigations with the organization's incident response capability.</p> <p>SG.PE-4.4 Determine if the organization 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.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical intrusion alarm / surveillance equipment logs or records; physical access logs or records; Smart Grid information system design documentation; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with physical access monitoring responsibilities].</p> <p>Test: [SELECT FROM: Physical access monitoring capability; Automated mechanisms implementing physical access monitoring capability].</p>
SG.PE-5	Visitor Control	<p>SG.PE-5.1 Determine if: (i) the organization documents physical access to the Smart Grid information system; (ii) the organization controls physical access to the Smart Grid information system by authenticating visitors before authorizing access to the facility.</p> <p>SG.PE-5.2 (requirement enhancement 1) Determine if: (i) the organization documents that visitors are escorted and required to adhere to the organization's security policies and procedures; (ii) the organization escorts visitors as required according to security policies and procedures; (iii) the organization monitors visitor activity as required according to security policies and procedures.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with visitor access control responsibilities].</p> <p>Test: [SELECT FROM: Visitor access control capability].</p>
SG.PE-6	Visitor Records	SG.PE-6.1 Determine if:	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing facility access records];

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(i) the organization maintains visitor access records to the facility that include: a) Name and organization of the person visiting; b) Signature of the visitor; c) Form of identification; d) Date of access; e) Time of entry and departure; f) Purpose of visit; and g) Name and organization of person visited. (ii) the organization documents designated officials within the organization to review the access logs after closeout and periodically review access logs based on an organization-defined frequency; (iii) designated officials within the organization to review the access logs after closeout and periodically review access logs based on an organization-defined frequency.		security plan; facility access control records; automated mechanisms supporting management of access records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing physical access records].
SG.PE-7	Physical Access Log Retention	SG.PE-7.1 Determine if 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.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; automated mechanisms supporting management of access records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing physical access records].
SG.PE-8	Emergency Shutoff Protection	SG.PE-8.1 Determine if the organization protects the emergency power-off capability from accidental and intentional/unauthorized activation.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to Smart Grid information system facility].
SG.PE-9	Emergency Power	SG.PE-9.1 Determine if 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.  SG.PE-9.2 (requirement enhancement 1) Determine if 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.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; alternate power supply documentation; alternate power test records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to Smart Grid information system facility].  Test: [SELECT FROM: Uninterruptible power supply; Alternate

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PE-10	Delivery and Removal	SG.PE-10.1 Determine if: (i) the organization authorizes organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items; (ii) the organization monitors organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items; (iii) the organization controls organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items.	Examine, Interview, Test	power supply]. Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing delivery and removal of Smart Grid information system components from the facility; security plan; facility housing the Smart Grid information system; records of items entering and exiting the facility; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with responsibilities for controlling Smart Grid information system components entering and exiting the facility]. Test: [SELECT FROM: Process for controlling Smart Grid information system-related items entering and exiting the facility].
SG.PE-11	Alternate Work Site	SG.PE-11.1 Determine if the organization 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. SG.PE-11.2 Determine if: (i) the organization implements appropriate management security measures at alternate control centers; (ii) the organization implements appropriate operational security measures at alternate control centers; (iii) the organization implements appropriate technical security measures at alternate control centers.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; security plan; list of management, operational, and technical security controls required for alternate work sites; assessments of security controls at alternate work sites; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel using alternate work sites].
SG.PE-12	Location of Smart Grid information system Assets	SG.PE-12.1 Determine if the organization locates Smart Grid information system assets to minimize potential damage from physical and environmental hazards. SG.PG-12.2 (requirement enhancement 1) Determine if the organization considers the risk associated with physical and environmental hazards when planning new Smart Grid information system facilities or reviewing existing facilities.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing positioning of Smart Grid information system components; documentation providing the location and position of Smart Grid information system components within the facility; physical site planning documents; organizational assessment of risk, contingency plan; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with site selection responsibilities for the facility housing the Smart Grid information system].
<b>Planning (SG.PL)</b>				
SG.PL-1	Strategic Planning Policy and Procedures	SG.PL-1.1 Determine if: (i) the organization develops a documented security strategic planning policy;	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>(ii) the security strategic planning policy addresses security strategic planning as it related to protecting the organization’s personnel and assets and the following:                      a) purpose / objective                      b) scope                      c) roles and responsibilities                      d) coordination among organizational entities, and compliance;                      (iii) the security strategic planning policy addresses the scope to include all organizational staff, contractors, and third parties;                      (iv) the organization implements the security strategic planning procedures;                      (v) the organization reviews and updates the security strategic planning procedures on an organizational defined frequency.</p> <p>SG.PL-1.2                      Determine if:                      (i) the organization documents management’s commitment to ensure compliance with the organization’s security strategic planning;                      (ii) management commitment ensures compliance with the organization’s security strategic planning.</p> <p>SG.PL-1.3                      Determine if:                      (i) the security strategic planning policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and                      (ii) the security strategic planning procedures facilitate implementation of the security strategic planning security policy.</p> <p>SG.PL-1.4                      Determine if:                      (i) the organization defines the frequency of security strategic planning policy and procedures reviews/updates;                      (ii) the organization reviews/updates the security strategic planning policy and procedures in accordance with the organization-defined frequency.</p>		<p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>
SG.PL-2	Smart Grid information system Security Plan	<p>SG.PL-2.1                      Determine if the organization 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;</p>	Examine, Interview	<p>Examine: [SELECT FROM: Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the Smart Grid information system; records of security plan reviews and updates; access control policy; contingency planning policy; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organization personnel with security planning and plan implementation responsibilities for</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		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.  SG.PL-2.2 Determine if the organization reviews the security plan for the Smart Grid information system on an organization-defined frequency.  SG.PL-2.3 Determine if the organization 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.		the Smart Grid information system].
SG.PL-3	Rules of Behavior	SG.PL-3.1 Determine if: (i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to Smart Grid information system usage, which includes a) use of social networking sites b) posting information on commercial websites c) sharing of Smart Grid information system account information (ii) the organization make readily available a set of rules that describe user responsibilities and expected behavior with regard to Smart Grid information system usage; (iii) the organization receives a signed acknowledgement 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.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing rules of behavior for Smart Grid information system users; rules of behavior; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel who are authorized users of the Smart Grid information system and have signed rules of behavior].
SG.PL-4	Privacy Impact Assessment	SG.PL-4.1 Determine if the organization conducts a privacy impact assessment on Smart Grid information systems.  SG.PL-4.2 Determine if: (i) the privacy impact assessment is reviewed by an organizational management authority; (ii) the privacy impact assessment is approved by an organizational management authority.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing privacy impact assessments on the Smart Grid information system; privacy impact assessment; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel who have privacy responsibilities].
SG.PL-5	Security-Related Activity Planning	SG.PL-5.1 Determine if: (i) the organization plans 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	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing security-related activity planning for the Smart Grid information system; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		individuals; (ii) the organization 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.  SG.PL-5.1 Determine if the organizational planning and coordination includes both emergency and nonemergency (e.g., routine) situations.		
<b>Security Program Management (SG.PM)</b>				
SG.PM-1	Security Policy and Procedures	SG.PM-1.1 Determine if: (i) the organization develops and documents policy and procedure for the security management program; (ii) the organization implements policy and procedure for the security management program; (iii) the organization disseminates policy and procedure to appropriate elements within the organization for the security management program; (iv) the organization reviews the policy and procedure for the security management program on a defined frequency; (v) the security management program policy and procedures address <ul style="list-style-type: none"> <li>a) purpose</li> <li>b) scope</li> <li>c) roles and responsibilities</li> <li>d) management commitment</li> <li>e) coordination among organizational entities, and compliance.</li> </ul> SG.PM-1.2 Determine if: (i) the organization documents management's commitment ensures compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements.  SG.PM-1.3 Determine if the organization ensures that the security program security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.PM-2	Security Program Plan	SG.PM-2.1 Determine if the organization develops and disseminates an organization-wide security program plan that— <ul style="list-style-type: none"> <li>a) Provides an overview of the requirements for the security</li> </ul>	Examine, Interview	Examine: [SELECT FROM: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates;

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>program and a description of the security program management requirements in place or planned for meeting those program requirements;</p> <p>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;</p> <p>c) Includes roles, responsibilities, management accountability, coordination among organizational entities, and compliance; and</p> <p>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.</p> <p>SG.PM-2.2 Determine if the organization reviews the organization-wide security program plan on an organization-defined frequency.</p> <p>SG.PM-2.3 Determine if the organization revises the plan to address organizational changes and problems identified during plan implementation or security requirement assessments.</p>		<p>information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities for the information security program].</p>
SG.PM-3	Senior Management Authority	<p>SG.PM-3.1 Determine if 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.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Information security program policy; information security program plan; documentation addressing roles and responsibilities of the senior information security officer position; information security program mission statement; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational person appointed to the senior information security officer position].</p>
SG.PM-4	Security Architecture	<p>SG.PM-4.1 Determine if the organization develops security architecture with consideration for the resulting risk to</p> <p>a) organizational operations</p> <p>b) organizational assets</p> <p>c) individuals</p> <p>d) other organizations.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Information security program policy; enterprise architecture policy; procedures addressing information security-related aspects of enterprise architecture development; system development life cycle documentation; enterprise architecture documentation; enterprise security architecture documentation; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational person appointed to the senior information security officer position].</p>
SG.PM-5	Risk Management Strategy	<p>SG.PM-5.1 Determine if the organization develops a comprehensive strategy to manage Smart Grid information system operational and usage risk to</p> <p>a) organizational operations</p> <p>b) organizational assets</p>	Examine, Interview	<p>Examine: [SELECT FROM: Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		c) individuals d) other organizations.  SG.PM-5.2 Determine if the organization implements that comprehensive risk strategy consistently across the organization.		Interview: [SELECT FROM: Organizational personnel with risk management strategy development and implementation responsibilities].
SG.PM-6	Security Authorization to Operate Process	SG.PM-6.1 Determine if the organization manages (e.g., documents, tracks, and reports) the security state of organizational Smart Grid information systems through security authorization processes.  SG.PM-6.2 Determine if the organization fully integrates the security authorization to operate processes into an organization-wide risk management strategy.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security authorization responsibilities for Smart Grid information systems; organizational personnel with risk management responsibilities].
SG.PM-7	Mission / business Process Definition	SG.PM-7.1 Determine if the organization defines mission / business processes that include a) consideration for security organizational operations, organizational assets, and individuals; b) the resulting risk to organizational operations, organizational assets, and individuals.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; risk management policy; procedures addressing security categorization of organizational information and Smart Grid information systems; organizational mission / business processes; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with mission / business process definition responsibilities; organizational personnel with security categorization and risk management responsibilities for the information security program].
SG.PM-8	Management Accountability	SG.PM-8.1 Determine if the organization defines a framework of management accountability that establishes roles and responsibilities to a) approve cyber security policy b) assign security roles c) coordinate the implementation of cyber security across the organization.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities for the information security program].
<b>Personnel Security (SG.PS)</b>				
SG.PS-1	Personnel Security Policy and Procedures	SG.PS-1.1 Determine if the organization develops, implements, reviews, and	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>updates on an organization-defined frequency</p> <p>a) A documented personnel security policy that addresses—</p> <p>    1) The objectives, roles, and responsibilities for the personnel security program as it relates to protecting the organization's personnel and assets; and</p> <p>    2) The scope of the personnel security program as it applies to all of the organizational staff, contractors, and third parties; and</p> <p>b) Procedures to address the implementation of the personnel security policy and associated personnel protection requirements.</p> <p>SG.PS-1.2 Determine if:</p> <p>(i) the organization documents management commitment ensures compliance with the organization's security policy and other regulatory requirements;</p> <p>(ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements.</p> <p>SG.PS-1.3 Determine if the organization ensures that the personnel security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.</p>		<p>records].</p> <p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>
SG.PS-2	Position Categorization	<p>SG.PS-2.1 Determine if:</p> <p>(i) the organization assigns a risk designation to all positions;</p> <p>(ii) the organization establishes screening criteria for individuals filling designated risk positions;</p> <p>(iii) the organization reviews position risk designations;</p> <p>(iv) the organization revises position risk designations;</p> <p>(v) the organization determines the frequency of the review based on the organization's requirements or regulatory commitments.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].</p>
SG.PS-3	Personnel Screening	<p>SG.PS-3.1 Determine if:</p> <p>(i) the organization screens individuals requiring access to the Smart Grid information system before access is authorized;</p> <p>(ii) the organization maintains consistency between the screening process and organization-defined policy, regulations, guidance, and the criteria established for the risk designation of the assigned position.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].</p>
SG.PS-4	Personnel Termination	<p>SG.PS-4.1 Determine if:</p> <p>(i) the organization revokes logical and physical access to facilities and systems when an employee is terminated;</p> <p>(ii) the organization ensures that all organization-owned property is returned when an employee is terminated;</p> <p>(iii) the organization-owned documents relating to the Smart Grid</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of Smart Grid information system accounts; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>information system that are in the employee's possession are transferred to the new authorized owner.</p> <p>SG.PS-4.2 Determine if the organization's logical and physical access must be terminated at an organization-defined time frame for personnel terminated for cause.</p> <p>SG.PS-4.3 Determine if the organization ensures that during the individuals exit interview they understand any security constraints imposed by being a former employee and that proper accountability is achieved for all Smart Grid information system-related property.</p>		
SG.PS-5	Personnel Transfer	<p>SG.PS-5.1 Determine if: (i) the organization reviews logical 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; (ii) the organization reviews 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.</p> <p>SG.PS-5.2 Determine if: (i) the organization completes the logical access permission review within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources; (ii) the organization completes the physical access permission review within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of Smart Grid information system and facility access authorizations; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].</p>
SG.PS-6	Access Agreements	<p>SG.PS-6.1 Determine if: (i) the organization completes appropriate agreements for Smart Grid information system access before access is granted; (ii) the organization ensures the Smart Grid information system access agreements apply to all parties, including third parties and contractors, who require access to the Smart Grid information system.</p> <p>SG.PS-6.2 Determine if: (i) the organization reviews Smart Grid information system access</p>	Examine, Interview	<p>Examine: [SELECT FROM: Personnel security policy; procedures addressing access agreements for organizational information and Smart Grid information systems; security plan; access agreements; records of access agreement reviews and updates; signed nondisclosure agreements; personnel security criteria; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		agreements periodically; (ii) the organization updates Smart Grid information system access agreements periodically.  SG.PS-6.3 Determine if the organization requires the 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.		
SG.PS-7	Contractor and Third-Party Personnel Security	SG.PS-7.1 Determine if: (i) the organization enforces Smart Grid information system security requirements for contractor and third-party personnel; (ii) the organization monitors service provider behavior and compliance to Smart Grid information system security requirements.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; third-party providers].
SG.PS-8	Personnel Accountability	SG.PS-8.1 Determine if the organization employs a formal accountability process for personnel failing to comply with established security policies and procedures and identifies disciplinary actions for failing to comply.  SG.PS-8.2 Determine if the organization ensures that the accountability process complies with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-9	Personnel Roles	SG.PS-9.1 Determine if the organization provides employees, contractors, and third parties with expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel sanctions; third party policy; third party standards and procedures; rules of behavior; records of formal sanctions; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; Organizational personnel with third party security responsibilities].
<b>Risk Management and Assessment (SG.RA)</b>				
SG.RA-1	Risk Assessment Policy and Procedures	SG.RA-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency a) A documented risk assessment security policy that addresses 1) The objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and 2) 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	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		assessment security policy and associated risk assessment protection requirements.  SG.RA-1.2 Determine if: (i) the organization documents management commitment ensures compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements.  SG.RA-1.3 Determine if the organization ensures that the risk assessment policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.RA-2	Risk Management Plan	SG.RA-2.1 Determine if the organization develops a risk management plan.  SG.RA-2.2 Determine if: (i) the organization assigns a management authority to review and approve a risk management plan; (ii) a management authority reviews and approves the risk management plan.  SG.RA-2.3 Determine if: (i) the organization's risk-reduction mitigation measures are planned to ensure effectiveness of the organization's risk management plan; (ii) the organization's risk-reduction mitigation measures are implemented to ensure effectiveness of the organization's risk management plan; (iii) the organization's risk-reduction mitigation results are monitored to ensure effectiveness of the organization's risk management plan.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with risk management strategy development and implementation responsibilities].
SG.RA-3	Security Impact Level	SG.RA-3.1 Determine if the organization specifies the information and the Smart Grid information system impact levels.  SG.RA-3.2 Determine if the organization documents the impact level results (including supporting rationale) in the security plan for information and the Smart Grid information system.  SG.RA-3.3	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy; procedures addressing security categorization of organizational information and Smart Grid information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if the organization reviews the Smart Grid information system and information impact levels on an organization-defined frequency.		
SG.RA-4	Risk Assessment	<p>SG.RA-4.1 Determine if the organization conducts assessments of risk from</p> <ul style="list-style-type: none"> <li>a) the unauthorized access of information and Smart Grid information systems</li> <li>b) use of information and Smart Grid information systems</li> <li>c) disclosure of information and Smart Grid information systems</li> <li>d) disruption of information and Smart Grid information systems</li> <li>e) modification of information and Smart Grid information systems</li> <li>f) destruction of information and Smart Grid information systems.</li> </ul> <p>SG.RA-4.2 Determine if the organization 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.</p>	Examine, Interview	<p>Examine: [SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with risk assessment responsibilities].</p>
SG.RA-5	Risk Assessment Update	SG.RA-5.1 Determine if 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.	Examine, Interview	<p>Examine: [SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with risk assessment responsibilities].</p>
SG.RA-6	Vulnerability Assessment and Awareness	<p>SG.RA-6.1 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization monitors 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;</li> <li>(ii) the organization 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.</li> </ul> <p>SG.RA-6.2 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization analyzes vulnerability scan reports within an organization-defined time frame based on an assessment of risk;</li> <li>(ii) the organization remediates vulnerabilities within an organization-defined time frame based on an assessment of risk.</li> </ul>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; security plan; Smart Grid information system design documentation; list of unauthorized software; notifications or alerts of unauthorized software on organizational Smart Grid information systems; list of Smart Grid information system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; vulnerability scanning tools and techniques documentation; penetration test results; vulnerability scanning results; vulnerability scanning tools and techniques documentation; patch and vulnerability management records; records of updates to vulnerabilities scanned; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with risk assessment and vulnerability scanning responsibilities].</p> <p>Test: [SELECT FROM: Vulnerability scanning capability and</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>SG.RA-6.3 Determine if the organization 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.</p> <p>SG.RA-6.4 Determine if the organization updates the Smart Grid information system to address any identified vulnerabilities in accordance with organization's Smart Grid information system maintenance policy.</p> <p>SG.RA-6.5 Determine if the organization updates the list of Smart Grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported.</p> <p>SG.RA-6.6 (requirement enhancement 1) Determine if the organization employs vulnerability scanning tools that include the capability to update the list of Smart Grid information system vulnerabilities scanned.</p> <p>SG.RA-6.7 (requirement enhancement 2) Determine if the organization includes privileged access authorization to organization-defined Smart Grid information system components for selected vulnerability scanning activities to facilitate more thorough scanning.</p>		associated scanning tools].
<b>Smart Grid information system and Services Acquisition (SG.SA)</b>				
SG.SA-1	Smart Grid information system and Services Acquisition Policy and Procedures	<p>SG.SA-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency</p> <ul style="list-style-type: none"> <li>a) A documented Smart Grid information system and services acquisition security policy that addresses                             <ul style="list-style-type: none"> <li>1) The objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and</li> <li>2) The scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and</li> </ul> </li> <li>b) Procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements.</li> </ul> <p>SG.SA-1.2 Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization documents management commitment ensures compliance with the organization's security policy and other</li> </ul>	Examine, Interview	<p>Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements.  SG.SA-1.3 Determine if the organization ensures that the Smart Grid information system and services acquisition security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.SA-2	Security Policies for Contractors and Third Parties	SG.SA-2.1 Determine if the organization's external suppliers and contractors that have an impact on the security of Smart Grid information systems must meet the organization's policy and procedures.  SG.SA-2.2 Determine if: (i) the organization establishes procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the contract; (ii) the organization documents procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the contract.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy and procedures; Personnel security policy; procedures addressing personnel sanctions; third party policy; third party standards and procedures; rules of behavior; records of formal sanctions; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; Organizational personnel with third party security responsibilities; Organizational personnel with system and services acquisition responsibilities].
SG.SA-3	Life-Cycle Support	SG.SA-3.1 Determine if the organization manages the Smart Grid information system using a system development lifecycle methodology that includes security.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; Smart Grid information system development life cycle documentation; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with information security and system life cycle development responsibilities].
SG.SA-4	Acquisitions	SG.SA-4.1 Determine if the organization includes security requirements in Smart Grid information system acquisition contracts in accordance with applicable laws, regulations, and organization-defined security policies.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing the integration of information security requirements and / or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for Smart Grid information systems or services; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].
SG.SA-5	Smart Grid information system Documentation	SG.SA-5.1 Determine if the Smart Grid information system documentation includes a) how to configure the Smart Grid information system and the	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system documentation; Smart Grid information system design documentation; Smart Grid information system documentation

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Smart Grid information system's security features; b) install the Smart Grid information system and the Smart Grid information system's security features; c) use the Smart Grid information system and the Smart Grid information system's security features.  SG.SA-5.2 Determine if the organization obtains from the contractor/third-party, information describing the functional properties of the security controls employed within the Smart Grid information system.		including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent Smart Grid information system documentation; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system documentation responsibilities; organizational personnel operating, using, and / or maintaining the Smart Grid information system; Organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and / or maintaining the Smart Grid information system].
SG.SA-6	Software License Usage Restrictions	SG.SA-6.1 Determine if the organization uses software and associated documentation in accordance with contract agreements and copyright laws.  SG.SA-6.2 Determine if the organization controls the use of software and associated documentation protected by quantity licenses and copyrighted material.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; procedures addressing the integration of information security requirements and / or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for Smart Grid information systems or services; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system administration responsibilities; organizational personnel operating, using, and / or maintaining the Smart Grid information system].
SG.SA-7	User-Installed Software	SG.SA-7.1 Determine if the organization establishes policies and procedures to manage user installation of software.	Examine, Interview, Test	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the Smart Grid information system; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system administration responsibilities; organizational personnel operating, using, and / or maintaining the Smart Grid information system].  Test: [SELECT FROM: Enforcement of rules for user installed software on the Smart Grid information system; Smart Grid information system for prohibited software].
SG.SA-8	Security Engineering Principles	SG.SA-8.1 Determine if: (i) the organization applies security engineering principles in the a) specification of any Smart Grid information system; b) design of any Smart Grid information system;	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the Smart Grid information system; Smart Grid information system design documentation; security requirements and security

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		c) development of any Smart Grid information system; d) implementation of any Smart Grid information system. (ii) the organization's security engineering principles include: a) Ongoing secure development education requirements for all developers involved in the Smart Grid information system; b) Specification of a minimum standard for security; c) Specification of a minimum standard for privacy; d) Creation of a threat model for a Smart Grid information system; e) Updating of product specifications to include mitigations for threats discovered during threat modeling; f) Use of secure coding practices to reduce common security errors; g) Testing to validate the effectiveness of secure coding practices; h) Performance of a final security audit prior to authorization to operate to confirm adherence to security requirements; i) Creation of a documented and tested security response plan in the event vulnerability is discovered; j) Creation of a documented and tested privacy response plan in the event vulnerability is discovered; k) Performance of a root cause analysis to understand the cause of identified vulnerabilities.		specifications for the Smart Grid information system; penetration test and vulnerability scan reports; security test and evaluation results; authority to operate documentation; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system design, development, implementation, and modification responsibilities; Organizational personnel with system and services acquisition responsibilities; Smart Grid information system authorizing official].
SG.SA-9	Developer Configuration Management	SG.SA-9.1 Determine if the organization requires that Smart Grid information system developers/integrators document and implement a configuration management process that a) Manages changes to the Smart Grid information system during design, development, implementation, and operation; b) Controls changes to the Smart Grid information system during design, development, implementation, and operation; c) Tracks security flaws; d) Tracks security flaws; e) Includes organizational approval of changes.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer / integrator configuration management plan; security flaw tracking records; system change authorization records; Smart Grid information system configuration management plan; other relevant documents or records].  Interview: [SELECT FROM: Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].
SG.SA-10	Developer Security Testing	SG.SA-10.1 Determine if the Smart Grid information system developer creates a security test and evaluation plan.  SG.SA-10.2 Determine if the developer submits the plan to the organization for approval and implements the plan once written approval is obtained.  SG.SA-10.3	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator security testing; acquisition contracts and service level agreements; Smart Grid information system developer / integrator security test plans; records of developer / integrator security testing results for the Smart Grid information system; security flaw tracking records; vulnerability scanning results; Smart Grid information system risk assessment reports; acquisition documentation; acquisition contracts for Smart Grid information systems or services;

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if the developer documents the results of the testing and evaluation and submits them to the organization for approval.  SG.SA-10.4 Determine if: (i) the organization prohibits developmental security tests on the production Smart Grid information system; (ii) the organization enforces prohibiting developmental security tests on the production Smart Grid information system.		security test and evaluation plan; security test and evaluation results report; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with developer security testing responsibilities].
SG.SA-11	Supply Chain Protection	SG.SA-11.1 Determine if the organization protects against supply chain vulnerabilities employing requirements defined to protect the products and services from threats initiated against a) organizations, that provides products or services to the organization; b) people, that provides products or services to the organization; c) information, that provides products or services to the organization; d) resources, that provides products or services to the organization.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and / or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for Smart Grid information systems or services; acquisition contracts and service level agreements; list of supply chain threats; list of measures to be taken against supply chain threats; Smart Grid information system development life cycle documentation; due diligence reviews documentation; procedures addressing the baseline configuration of the Smart Grid information system; configuration management plan; Smart Grid information system design documentation; Smart Grid information system architecture and configuration documentation; penetration testing records; security test and evaluation results reports; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with supply chain protection responsibilities; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].
<b>Smart Grid information system and Communication Protection (SG.SC)</b>				
SG.SC-1	System and Communication Protection Policy and Procedures	SG.SC-1.1 Determine if 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— 1) 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 2) 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	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		and associated Smart Grid information system and communication protection requirements.  SG.SC-1.2 Determine if: (i) the organization documents management commitment ensures compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements.  SG.AC-1.3 Determine if 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.		
SG.SC-2	Communications Partitioning	SG.SC-2.1 Determine if the Smart Grid information system partitions the communications for telemetry/data acquisition services and management functionality.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; procedures addressing communication partitioning; procedures addressing quality of services; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel installing, configuring, and / or maintaining communications].
SG.SC-3	Security Function Isolation	SG.SC-3.1 Determine if the Smart Grid information system isolates security functions from nonsecurity functions.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; procedures addressing security function isolation; list of critical security functions; list of security functions to be isolated from nonsecurity functions; Smart Grid information system design documentation; hardware separation mechanisms; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Separation of security functions from nonsecurity functions within the Smart Grid information system; Hardware separation mechanisms facilitating security function isolation; Isolation of security functions enforcing access and information flow control].
SG.SC-4	Information Remnants	SG.SC-4.1 Determine if the Smart Grid information system prevents unauthorized or unintended information transfer via shared Smart Grid information system resources.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing information remnants; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Test: [SELECT FROM: Smart Grid information system for unauthorized and unintended transfer of information via shared system resources].
SG.SC-5	Denial-of-Service Protection	SG.SC-5.1 Determine if: (i) 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; (ii) the organization documents a defined list of denial-of-service attacks against the Smart Grid information systems.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing denial of service protection; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Smart Grid information system for protection against or limitation of the effects of denial of service attacks; Automated mechanisms implementing Smart Grid information system bandwidth, capacity, and redundancy management].
SG.SC-6	Resource Priority	SG.SC-6.1 Determine if the Smart Grid information system prioritizes the use of resources.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing prioritization of Smart Grid information system resources; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing resource allocation capability].
SG.SC-7	Boundary Protection	SG.SC-7.1 Determine if the organization defines the boundary of the Smart Grid information system.  SG.SC-7.2 Determine if: (i) the Smart Grid information system monitors communications at the external boundary of the system and at key internal boundaries within the system; (ii) the Smart Grid information system controls communications at the external boundary of the system and at key internal boundaries within the system.  SG.SC-7.3 Determine if the Smart Grid information system connects to external networks or Smart Grid information systems only through managed interfaces consisting of boundary protection devices.  SG.SC-7.4 Determine if the managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the Smart Grid information system; list of mediation vehicles for allowing public access to the organization's internal networks; Smart Grid information system design documentation; boundary protection hardware and software; traffic flow policy; Smart Grid information system security architecture; boundary protection hardware and software; records of traffic flow policy exceptions; Smart Grid information system hardware and software; Smart Grid information system architecture; Smart Grid information system configuration settings and associated documentation; facility communications and wiring diagram; Smart Grid information system architecture; Smart Grid information system audit records; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific boundary ownership and responsibilities].  Test: [SELECT FROM: Automated mechanisms implementing boundary protection capability within the Smart Grid information system; Automated mechanisms implementing

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>SG.SC-7.5 Determine if the organization prevents public access into the organization's internal Smart Grid information system networks except as appropriately mediated.</p> <p>SG.SC-7.6 (requirement enhancement 1) Determine if: (i) the Smart Grid information system denies network traffic by default; (ii) the Smart Grid information system allows network traffic by exception.</p> <p>SG.SC-7.7 (requirement enhancement 2) Determine if 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.</p> <p>SG.SC-7.8 (requirement enhancement 3) Determine if: (i) communications to/from Smart Grid information system components shall be restricted to specific components in the Smart Grid information system; (ii) communications shall restricted to/from any non-Smart Grid information system unless separated by a controlled logical/physical interface.</p>		<p>access controls for public access to the organization's internal networks; Managed interfaces implementing organizational traffic flow policy; Automated mechanisms supporting the fail-safe boundary protection capability within the Smart Grid information system; Automated mechanisms supporting non-remote connections with the Smart Grid information system; Mechanisms implementing managed interfaces within Smart Grid information system boundary protection devices; Automated mechanisms preventing unauthorized exfiltration of information across managed interfaces; Automated mechanisms implementing host-based boundary protection capability; Physical access capability implementing protections against unauthorized physical connections to the Smart Grid information system; Mechanisms routing networked, privileged access through dedicated managed interfaces; Mechanisms preventing discovery of system components at a managed interface].</p>
SG.SC-8	Communication Integrity	<p>SG.SC-8.1 Determine if the Smart Grid information system protects the integrity of electronically communicated information.</p> <p>SG.SC-8.2 (requirement enhancement 1) Determine if the organization employs cryptographic mechanisms to ensure integrity of Smart Grid information system information.</p>	Examine, Test	<p>Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].</p> <p>Test: [SELECT FROM: Transmission integrity capability within the Smart Grid information system; Cryptographic mechanisms implementing transmission integrity capability within the Smart Grid information system; Transmission integrity capability within the Smart Grid information system].</p>
SG.SC-9	Communication Confidentiality	<p>SG.SC-9.1 Determine if the Smart Grid information system protects the confidentiality of communicated information.</p> <p>SG.SC-9.2 (requirement enhancement 1) Determine if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission of Smart Grid information system information.</p>	Examine, Test	<p>Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality; Smart Grid information system design documentation; Smart Grid information system communications hardware and software or Protected Distribution System protection mechanisms; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Test: [SELECT FROM: Cryptographic mechanisms implementing transmission confidentiality capability within the Smart Grid information system; Transmission confidentiality capability within the Smart Grid information system; Transmission confidentiality capability within the Smart Grid information system].
SG.SC-10	Trusted Path	SG.SC-10.1 Determine if: (i) the Smart Grid information system establishes a trusted communications path between the user and the Smart Grid information system. (ii) the Smart Grid information system documents trusted communications path between the user and the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing trusted communications paths; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing trusted communications paths within the Smart Grid information system].
SG.SC-11	Cryptographic Key Establishment and Management	SG.SC-11.1 Determine if: (i) the organization establishes cryptographic keys for required cryptography employed within the Smart Grid information system; (ii) the organization manages cryptographic keys for required cryptography employed within the Smart Grid information system.  SG.SC-11.2 (requirement enhancement 1) Determine if: (i) the key establishment includes a key generation process in accordance with a specified algorithm and key sizes, and key sizes based on an assigned standard; (ii) the key generation must be performed using an appropriate random number generator; (iii) the policies for key management need to address such items as periodic key changes, key destruction, and key distribution.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing cryptographic key management and establishment; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for cryptographic key establishment or management].  Test: [SELECT FROM: Automated mechanisms implementing cryptographic key management and establishment within the Smart Grid information system].
SG.SC-12	Use of Validated Cryptography	SG.SC-12.1 Determine if: (i) the organization documents all of the cryptography and other cryptographic security functions (e.g., hashes, random number generators, etc.) that are required for use in a Smart Grid information system; (ii) all cryptography and other cryptographic security functions shall be NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; cryptographic module validation certificates; cryptographic module validation certificates; NIST cryptographic standards; FIPS cryptographic module validation certificates; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for implementing cryptography within the

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Smart Grid information system]. Test: [SELECT FROM: Automated mechanisms implementing cryptographic key management and establishment within the Smart Grid information system].
SG.SC-13	Collaborative Computing	SG.SC-13.1 Determine if: (i) the organization develops an organization-defined frequency a collaborative computing policy; (ii) the organization disseminates an organization-defined frequency a collaborative computing policy; (iii) the organization periodically reviews on an organization-defined frequency a collaborative computing policy; (iv) the organization periodically updates on an organization-defined frequency a collaborative computing policy.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].
SG.SC-14	Transmission of Security Parameters	SG.SC-14.1 Determine if the Smart Grid information system reliably associates security parameters with information exchanged between the enterprise Smart Grid information systems and the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission of security parameters; access control policy and procedures; boundary protection procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms supporting reliable transmission of security parameters between Smart Grid information systems].
SG.SC-15	Public Key Infrastructure Certificates	SG.SC-15.1 Determine if 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.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with public key infrastructure certificate issuing responsibilities].  Test: [SELECT FROM: Automated mechanisms supporting reliable transmission of security parameters between Smart Grid information systems through the use of public key infrastructures].
SG.SC-16	Mobile Code	SG.SC-16.1 Determine if: (i) the organization establishes usage restrictions for mobile code technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; (ii) the organization establishes implementation guidance for mobile code technologies based on the potential to cause damage to	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		the Smart Grid information system if used maliciously.  SG.SC-16.2 Determine if the organization a) documents the use of mobile code within the Smart Grid information system; b) monitors the use of mobile code within the Smart Grid information system; c) manages the use of mobile code within the Smart Grid information system.  SG.SC-16.3 Determine if: (i) the organization documents a management authority to authorize the use of mobile code; (ii) a management authority authorizes the use of mobile code.		documentation; Smart Grid information system audit records; acquisition documentation; acquisition contracts for Smart Grid information systems or services; list of applications for which automatic execution of mobile code must be prohibited; list of actions required before execution of mobile code; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with mobile code authorization, monitoring, and control responsibilities; Organizational personnel with mobile code management responsibilities; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].  Test: [SELECT FROM: Mobile code authorization and monitoring capability for the organization; Automated mechanisms implementing mobile code detection and inspection capability; Automated mechanisms preventing download and execution of prohibited mobile code; Automated mechanisms preventing mobile code execution within the Smart Grid information system].
SG.SC-17	Voice-Over Internet Protocol	SG.SC-17.1 Determine if: (i) the organization establishes usage restrictions for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; (ii) the organization establishes implementation guidance for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously.  SG.SC-17.2 Determine if the organization a) authorizes the use of VoIP within the Smart Grid information system; b) monitors the use of VoIP within the Smart Grid information system; c) controls the use of VoIP within the Smart Grid information system.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with VoIP authorization and monitoring responsibilities].  Test: [SELECT FROM: VoIP authorization and monitoring capability for the organization].
SG.SC-18	System Connections	SG.SC-18.1 Determine if: (i) the organization documents all external Smart Grid information system and communication connections; (ii) the organization protects all external Smart Grid information system and communication connections from tampering or damage.	Examine, Interview	Examine: [SELECT FROM: Access control policy; procedures addressing Smart Grid information system connections; system and communications protection policy; Smart Grid information system interconnection security agreements; security plan; Smart Grid information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Interview: [SELECT FROM: Organizational personnel with responsibility for developing, implementing, or approving Smart Grid information system interconnection agreements].
SG.SC-19	Security Roles	SG.SC-19.1 Determine if: (i) the Smart Grid information system design specifies the security roles and responsibilities for the users of the Smart Grid information system; (ii) the Smart Grid information system implementation specifies the security roles and responsibilities for the users of the Smart Grid information system	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer / integrator configuration management plan; security flaw tracking records; system change authorization records; Smart Grid information system configuration management plan; other relevant documents or records].  Interview: [SELECT FROM: Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].
SG.SC-20	Message Authenticity	SG.SC-20.1 Determine if the Smart Grid information system provides mechanisms to protect the authenticity of device-to-device communications.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Transmission integrity capability within the Smart Grid information system; Cryptographic mechanisms implementing transmission integrity capability within the Smart Grid information system; Transmission integrity capability within the Smart Grid information system].
SG.SC-21	Secure Name/Address Resolution Service	SG.SC-21.1 Determine if the organization is responsible for a) 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; b) 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.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing secure name/address resolution service (authoritative source); Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services].
SG.SC-22	Fail in Known State	SG.SC-22.1 Determine if: (i) the Smart Grid information system fails to a known state for defined failures; (ii) the organization documents what fails to a known state for defined failures consists of.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing Smart Grid information system failure; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of failures requiring Smart Grid information system to fail in a

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				known state; state information to be preserved in system failure; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing fail-in-known-state capability].
SG.SC-23	Thin Nodes	SG.SC-23.1 Determine if the Smart Grid information system employs processing components that have minimal functionality and data storage.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of thin nodes; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].
SG.SC-24	Honeypots	SG.SC-24.1 Determine if the Smart Grid information system includes components specifically designed to be the target of malicious attacks for the purpose of a) detecting b) deflecting c) analyzing d) tracking attacks.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of honeypots; access control policy and procedures; boundary protection procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms proactively seeking Web-based malicious code].
SG.SC-25	Operating System-Independent Applications	SG.SC-25.1 Determine if the Smart Grid information system includes organization-defined applications that are independent of the operating system.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing operating system-independent applications; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of operating system-independent applications; other relevant documents or records].
SG.SC-26	Confidentiality of Information at Rest	SG.SC-26.1 Determine if 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.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing protection of information at rest; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records].  Test: [SELECT FROM: Automated mechanisms implementing confidentiality and integrity protections for information at-rest; Cryptographic mechanisms implementing confidentiality and integrity protections for information at-rest].
SG.SC-27	Heterogeneity	SG.SC-27.1 Determine if the organization employs diverse technologies in the implementation of the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of technologies deployed in the Smart Grid information system; acquisition documentation; acquisition contracts for Smart Grid

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				information system components or services; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with Smart Grid information system acquisition, development, and implementation responsibilities].
SG.SC-28	Virtualization Technique	SG.SC-28.1 Determine if 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.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system architecture; list of virtualization techniques to be employed for organizational Smart Grid information systems; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with responsibilities for implementing approved virtualization techniques for Smart Grid information systems].
SG.SC-29	Application Partitioning	SG.SC-29.1 Determine if the Smart Grid information system separates user functionality (including user interface services) from Smart Grid information system management functionality.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing application partitioning; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Separation of user functionality from Smart Grid information system management functionality].
SG.SC-30	Smart Grid information system Partitioning	SG.SC-30.1 Determine if the organization partitions the Smart Grid information system into components residing in separate physical or logical domains (or environments).	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system architecture; list of Smart Grid information system physical domains (or environments); Smart Grid information system facility diagrams; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel installing, configuring, and / or maintaining the Smart Grid information system].
<b>Smart Grid information system and Information Integrity (SG.SI)</b>				
SG.SI-1	System and Information Integrity Policy and Procedures	SG.SI-1.1 Determine if: (i) the organization develops and implements a documented Smart Grid information and integrity policy; (ii) the Smart Grid information and integrity policy addresses Smart Grid information and integrity as it related to protecting the organization's personnel and assets and the following: a) purpose / objective	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		<p>b) scope                      c) roles and responsibilities                      d) coordination among organizational entities, and compliance;                      (iii) the Smart Grid information and integrity policy addresses the scope to include all organizational staff, contractors, and third parties;                      (iv) the organization develops and implements the Smart Grid information and integrity procedures;                      (v) the organization reviews and updates the Smart Grid information and integrity procedures;                      (vi) management commitment ensures compliance with the organization's access control;                      (vii) the Smart Grid information and integrity policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and                      (viii) the Smart Grid information and integrity procedures facilitate implementation of the Smart Grid information and integrity security policy.</p> <p>SG.SI-1.2                      Determine if:                      (i) the organization defines the frequency of Smart Grid information and integrity policy and procedures reviews/updates;                      (ii) the organization reviews/updates the Smart Grid information and integrity policy and procedures in accordance with the organization-defined frequency.</p>		
SG.SI-2	Flaw Remediation	<p>SG.SI-2.1                      Determine if:                      (i) the organization identifies Smart Grid information system flaws;                      (ii) the organization reports Smart Grid information system flaws;                      (iii) the organization corrects Smart Grid information system flaws.</p> <p>SG.SI-2.2                      Determine if the organization tests software updates related to flaw remediation for effectiveness and potential side effects on organizational Smart Grid information systems before installation.</p> <p>SG.SI-2.3                      Determine if the organization incorporates flaw remediation into the organizational configuration management process.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the Smart Grid information system; list of recent security flaw remediation actions performed on the Smart Grid information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct Smart Grid information system flaws); test results from the installation of software to correct Smart Grid information system flaws; Automated mechanisms supporting centralized management of flaw remediation and automatic software updates; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of Smart Grid information system flaws; list of recent security flaw remediation actions performed on the Smart Grid information system; Smart Grid information system audit records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with flaw remediation responsibilities].</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				<p>Test: [SELECT FROM: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates; Automated mechanisms implementing Smart Grid information system flaw remediation update status; Automated mechanisms facilitating flaw remediation to Smart Grid information system components].</p>
SG.SI-3	Malicious Code and Spam Protection	<p>SG.SI-3.1 Determine if: (i) the organization implements malicious code protection mechanisms; (ii) the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.</p> <p>SG.SI-3.2 Determine if the Smart Grid information system prevents users from circumventing malicious code protection capabilities.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; procedures addressing spam protection; spam protection mechanisms; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with malicious code protection responsibilities; Organizational personnel with spam protection responsibilities].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing malicious code protection capability; Automated mechanisms implementing spam detection and handling capability].</p>
SG.SI-4	Smart Grid information system Monitoring Tools and Techniques	SG.SI-4.1 Determine if the organization monitors events on the Smart Grid information system to detect attacks, unauthorized activities or conditions, and non-malicious errors.	Examine, Interview, Test	<p>Examine: [SELECT FROM: System and information integrity policy; procedures addressing Smart Grid information system monitoring tools and techniques; Smart Grid information system design documentation; Smart Grid information system monitoring tools and techniques documentation; Smart Grid information system configuration settings and associated documentation; techniques; documentation providing evidence of testing intrusion monitoring tools; Smart Grid information system monitoring tools and techniques documentation; list of common traffic patterns and / or events; Smart Grid information system protocols documentation; list of acceptable thresholds for false positives and false negatives; event correlation logs or records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with Smart Grid information system monitoring responsibilities].</p> <p>Test: [SELECT FROM: Smart Grid information system-wide intrusion detection capability; Automated tools supporting near real-time event analysis; Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms; Smart Grid information system monitoring real-time alert capability; Smart Grid information system-wide</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				intrusion detection and prevention capability; Smart Grid information system notification capability; Automated mechanisms implementing alerts to security personnel for inappropriate or unusual activities; Automated mechanisms implementing wireless communications intrusion detection capability].
SG.SI-5	Security Alerts and Advisories	<p>SG.SI-5.1 Determine if the organization receives Smart Grid information system security alerts, advisories, and directives from external organizations.</p> <p>SG.SI-5.2 Determine if: (i) the organization generates internal security alerts, advisories, and directives as deemed necessary; (ii) the organization disseminates internal security alerts, advisories, and directives as deemed necessary.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the Smart Grid information system].</p> <p>Test: [SELECT FROM: Automated mechanisms implementing the distribution of security alert and advisory information].</p>
SG.SI-6	Security Functionality Verification	<p>SG.SI-6.1 Determine if 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.</p> <p>SG.SI-6.2 Determine if the Smart Grid information system notifies the management authority when anomalies are discovered.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: System and information integrity policy; procedures addressing security function verification; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; automated security test results; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Organizational personnel with security functionality verification responsibilities; organizational personnel with information security responsibilities].</p> <p>Test: [SELECT FROM: Security function verification capability; Automated mechanisms implementing alerts and / or notifications for failed automated security tests; mated mechanisms supporting the management of distributed security function testing].</p>
SG.SI-7	Software and Information Integrity	<p>SG.SI-7.1 Determine if: (i) the Smart Grid information system monitors unauthorized changes to software and information; (ii) the Smart Grid information system detects unauthorized changes to software and information.</p>	Examine, Interview, Test	<p>Examine: [SELECT FROM: System and information integrity policy; procedures addressing software and information integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; integrity verification tools and applications documentation; automated tools supporting alerts</p>

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.SI-7.2 (Requirement enhancement 1) Determine if: (i) the organization reassesses the integrity of software by performing on an organization-defined frequency integrity scans of the Smart Grid information system; (ii) the organization reassesses the integrity of information by performing on an organization-defined frequency integrity scans of the Smart Grid information system; (iii) the organization defines the frequency of the integrity scans of the Smart Grid information systems.		and notifications for integrity discrepancies; records of integrity scans; Smart Grid information system component packaging; other relevant documents or records].  Interview: [SELECT FROM: Organizational personnel with security functionality verification responsibilities; organizational personnel with software integrity responsibilities; organization responsibility with change management responsibilities; organizational personnel with information security responsibilities].  Test: [SELECT FROM: Software integrity protection and verification capability].
SG.SI-8	Information Input Validation	SG.SI-8.1 Determine if: (i) the Smart Grid information system employs mechanisms to check information for accuracy; (ii) the Smart Grid information system employs mechanisms to check information for completeness; (iii) the Smart Grid information system employs mechanisms to check information for validity; (iv) the Smart Grid information system employs mechanisms to check information for authenticity.	Examine, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing information validity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify validity of information; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Smart Grid information system capability for checking validity of information inputs].
SG.SI-9	Error Handling	SG.SI-9.1 Determine if the Smart Grid information system identifies error conditions.  SG.SI-9.2 Determine if the Smart Grid information system generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries.	Examine, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing Smart Grid information system error handling; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records].  Test: [SELECT FROM: Smart Grid information system error handling capability].

655  
656