

# Companion Spreadsheet to the NISTIR 7628 Assessment Guide Validation/Review Process

*Please email Nelson and Vicky if interested in reviewing a NISTIR 7628 Family (or two... or three...)*

## 1. NISTIR 7628 High-Level Requirement

<b>SG.AC-2 Remote Access Policy and Procedures</b>		
Category: Common Governance, Risk, and Compliance (GRC) Requirements		
<b>Requirement</b>		
The organization—		
1. Documents allowed methods of remote access to the Smart Grid information system;		
2. Establishes usage restrictions and implementation guidance for each allowed remote access method;		
3. Authorizes remote access to the Smart Grid information system prior to connection; and		
4. Enforces requirements for remote connections to the Smart Grid information system.		
<b>Supplemental Guidance</b>		
Remote access is any access to an organizational Smart Grid information system by a user (or process acting on behalf of a user) communicating through an external, non-organization-controlled network (e.g., the Internet).		
<b>Requirement Enhancements</b>		
None.		
<b>Additional Considerations</b>		
None.		
<b>Impact Level Allocation</b>		
Low: SG.AC-2	Moderate: SG.AC-2	High: SG.AC-2

## 2. Mapping to NIST SP 800-53 Control *(Please include a note to Vicky [pillitteri\\_victoria@bah.com](mailto:pillitteri_victoria@bah.com) if there are any identified typos, omissions, missing/incorrect mappings in the NISTIR 7628 High-Level Requirements)*

### APPENDIX A CROSSWALK OF CYBER SECURITY DOCUMENTS

Table A-1 Crosswalk of Cyber Security Requirements and Documents

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) May 2009
Dark Gray = Unique Technical Requirement      Light Gray = Common Technical Requirement White = Common Governance, Risk and Compliance (GRC)						
<b>Access Control (SG.AC)</b>						
SG.AC-1	Access Control Policy and Procedures	AC-1	Access Control Policy and Procedures	2.15.1	Access Control Policies and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)
<b>SG.AC-2</b>	Remote Access Policy and Procedures	AC-17	Remote Access	2.15.23	Remote Access Policy and Procedures	CIP005-2 (R1, R1.1, R1.2, R2, R2.3, R2.4)
SG.AC-3	Account Management	AC-2	Account Management	2.15.3	Account Management	CIP 003-2 (R5, R5.1, R5.2, R5.3) CIP 004-2 (R4, R4.1, R4.2) CIP 005-2 (R2.5) CIP 007-2 (R5, R5.1, R5.2)
SG.AC-4	Access Enforcement	AC-3	Access Enforcement	2.15.7	Access Enforcement	CIP 004-2 (R4) CIP 005-2 (R2, R2.1-R2.4)
SG.AC-5	Information Flow Enforcement	AC-4	Information Flow Enforcement	2.15.15	Information Flow Enforcement	



### 3. Review corresponding NIST SP 800-53 Control

#### AC-17 REMOTE ACCESS

Control: The organization:

- a. Documents allowed methods of remote access to the information system;
- b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
- c. Monitors for unauthorized remote access to the information system;
- d. Authorizes remote access to the information system prior to connection; and
- e. Enforces requirements for remote connections to the information system.

Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external

networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.

#### Control Enhancements:

- (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

- (2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13.

- (3) The information system routes all remote accesses through a limited number of managed access control points.

Enhancement Supplemental Guidance: Related control: SC-7.

- (4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

Enhancement Supplemental Guidance: Related control: AC-6.

- (5) The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.
- (6) The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
- (7) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited.

Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.

- (8) The organization disables [Assignment: organization-defined networking protocols within the information system deemed to be nonsecure] except for explicitly identified components in support of specific operational requirements.

Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

Priority and Baseline Allocation:

P1	LOW AC-17	MOD AC-17 (1) (2) (3) (4) (5) (7) (8)	HIGH AC-17 (1) (2) (3) (4) (5) (7) (8)
----	-----------	---------------------------------------	--

- Identify corresponding portions of NISTIR 7628 and 800-53 requirements (see text that is “boxed” in matching colors)
- For corresponding portions of 800-53 requirements, identify corresponding portions of assessment objectives/methods in 800-53A (see text that is also boxed in the same color).

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

ASSESSMENT PROCEDURE	
AC-17	REMOTE ACCESS
AC-17.1	<p><b>ASSESSMENT OBJECTIVE:</b> Determine if:</p> <p>(i) the organization documents allowed methods of remote access to the information system;</p> <p>(ii) the organization establishes usage restrictions and implementation guidance for each allowed remote access method;</p> <p>(iii) the organization monitors for unauthorized remote access to the information system;</p> <p>(iv) the organization authorizes remote access to the information system prior to connection; and</p> <p>(v) the organization enforces requirements for remote connections to the information system.</p> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b>            Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].            Interview: [SELECT FROM: Organizational personnel with remote access authorization, monitoring, and control responsibilities].            Test: [SELECT FROM: Remote access methods for the information system].</p>

AC-17(1)	REMOTE ACCESS
AC-17(1).1	<p><b>ASSESSMENT OBJECTIVE:</b> Determine if the organization employs automated mechanisms to facilitate and control of remote access methods.</p> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b>            Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records].            Test: [SELECT FROM: Automated mechanisms implementing the access control policy access].</p>

Note that NIST SP 800-53 (and 800-53A) may have additional controls and control enhancements not in the NISTIR 7628.

AC-17(2)	REMOTE ACCESS
AC-17(2).1	<p><b>ASSESSMENT OBJECTIVE:</b>  <i>Determine if the organization uses cryptography to protect the confidentiality and integrity of remote access sessions.</i></p> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b>  <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  <b>Test:</b> [SELECT FROM: Automated mechanisms implementing cryptographic protections for remote access].</p>

AC-17(3)	REMOTE ACCESS
AC-17(3).1	<p><b>ASSESSMENT OBJECTIVE:</b>  <i>Determine if:</i></p> <ul style="list-style-type: none"> <li>(i) <i>the organization defines a limited number of managed access control points for remote access to the information system; and</i></li> <li>(ii) <i>the information system routes all remote accesses through managed access control points.</i></li> </ul> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b>  <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  <b>Test:</b> [SELECT FROM: Automated mechanisms implementing the access control policy for remote access].</p>

AC-17(4)	REMOTE ACCESS
AC-17(4).1	<p><b>ASSESSMENT OBJECTIVE:</b>  <i>Determine if:</i></p> <ul style="list-style-type: none"> <li>(i) <i>the organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and</i></li> <li>(ii) <i>the organization documents the rationale for such access in the security plan for the information system.</i></li> </ul> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b>  <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records].</p>

AC-17(5)	REMOTE ACCESS
AC-17(5).1	<p><b>ASSESSMENT OBJECTIVE:</b>  <i>Determine if:</i></p> <ul style="list-style-type: none"> <li>(i) <i>the organization defines the frequency of monitoring for unauthorized remote connections to the information system;</i></li> <li>(ii) <i>the organization monitors for unauthorized remote connections to the information system in accordance with the organization-defined frequency;</i></li> <li>(iii) <i>the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered; and</i></li> <li>(iv) <i>the organization takes organization-defined appropriate action(s) if an unauthorized connection is discovered.</i></li> </ul> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b>  <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  <b>Interview:</b> [SELECT FROM: Organizational personnel with responsibilities for monitoring remote connections to the information system].</p>

AC-17(6)	REMOTE ACCESS
AC-17(6).1	<p><b>ASSESSMENT OBJECTIVE:</b>  <i>Determine if the organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.</i></p> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b>  <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access to the information system; other relevant documents or records].  <b>Interview:</b> [SELECT FROM: Organizational personnel with responsibilities for implementing or monitoring remote access to the information system; information system users with knowledge of information about remote access mechanisms].</p>

AC-17(7)	REMOTE ACCESS
AC-17(7).1	<p><b>ASSESSMENT OBJECTIVE:</b> Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization defines the security functions and security-relevant information that can be accessed using remote sessions;</li> <li>(ii) the organization defines the additional security measures to be employed for remote sessions used to access organization-defined security functions and security-relevant information;</li> <li>(iii) the organization employs organization-defined additional security measures for remote sessions used to access organization-defined security functions and security-relevant information; and</li> <li>(iv) the organization audits remote sessions for accessing organization-defined security functions and security-relevant information.</li> </ul> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b> Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for remote access].</p>

AC-17(8)	REMOTE ACCESS
AC-17(8).1	<p><b>ASSESSMENT OBJECTIVE:</b> Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization defines the networking protocols within the information system deemed to be nonsecure; and</li> <li>(ii) the organization disables the organization-defined networking protocols within the information system deemed to be nonsecure except for explicitly identified components in support of specific operational requirements.</li> </ul> <p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b> Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; security plan; list of networking protocols deemed to be non-secure; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms disabling networking protocols deemed to be non-secure].</p>

6. Based on the NISTIR 7628 to NIST SP 800-53 to NIST SP 800-53A relationship, **validate the content columns E, F and G in the Companion Spreadsheet** (which will also change Appendix B in the Assessment Guide)
  - a. Identify text to be **REMOVED in BLUE (or BLUE-STRIKETROUGH)**
  - b. Identify text to be **ADDED in RED**

	E	F	G
SG.AC-2.1	<p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the Smart Grid information system is allowed;</li> <li>(ii) the organization documents the allowed remote access to the Smart Grid information system;</li> <li>(iii) <del>the organization establishes usage restrictions and implementation guidance for each allowed remote access method;</del></li> <li>(iv) the organization authorizes remote access to the Smart Grid information system prior to connection; and</li> <li>(v) the organization enforces requirements for remote connections to Smart Grid information systems.</li> </ul>	Examine, Interview, Test	<p>Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the Smart Grid information system; information system configuration settings and associated documentation; Smart Grid information system audit records; 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> <p>Test: [SELECT FROM: Remote access methods for the Smart Grid information system].</p>
SG.AC-2.2	<p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization defines managed access control points for remote access to the Smart Grid information system; and</li> <li>(ii) the Smart Grid information system controls all remote accesses through a limited number of managed access control points.</li> </ul>		