NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

The Smart Grid Interoperability Panel–Cyber Security Working Group

August 2010

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

APPENDIX A
CROSSWALK OF CYBER SECURITY DOCUMENTS

Table A-1 Crosswalk of Cyber Security Requirements and Documents

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
Access Control (SG.AC)						
SG.AC-1	Access Control Policy and Procedures	AC-1	Access Control Policy and Procedures	2.15.1	Access Control Policies and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)
SG.AC-2	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	
SG.AC-6	Separation of Duties	AC-5	Separation of Duties	2.15.8	Separation of Duties	
SG.AC-7	Least Privilege	AC-6	Least Privilege	2.15.9	Least Privilege	CIP 007-2 (R5.1)
SG.AC-8	Unsuccessful Login Attempts	AC-7	Unsuccessful Login Attempts	2.15.20	Unsuccessful Logon Notification	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
SG.AC-9	Smart Grid Information System Use Notification	AC-8	System Use Notification	2.15.17	System Use Notification	CIP 005-2 (R2.6)
SG.AC-10	Previous Logon Notification	AC-9	Previous Logon (Access) Notification	2.15.19	Previous Logon Notification	
SG.AC-11	Concurrent Session Control	AC-10	Concurrent Session Control	2.15.18	Concurrent Session Control	
SG.AC-12	Session Lock	AC-11	Session Lock	2.15.21	Session Lock	
SG.AC-13	Remote Session Termination			2.15.22	Remote Session Termination	
SG.AC-14	Permitted Actions without Identification or Authentication	AC-14	Permitted Actions without Identification or Authentication	2.15.11	Permitted Actions without Identification and Authentication	
SG.AC-15	Remote Access	AC-17	Remote Access	2.15.24	Remote Access	CIP 005-2 (R2, R3, R3.1, R3.2)
SG.AC-16	Wireless Access Restrictions			2.15.26	Wireless Access Restrictions	
SG.AC-17	Access Control for Portable and Mobile Devices	AC-19	Access Control for Mobile Devices	2.15.25	Access Control for Portable and Mobile Devices	CIP 005-2 (R2.4, R5, R5.1)
SG.AC-18	Use of External Information Control Systems	SC-7	Boundary Protection	2.15.29	Use of External Information Control Systems	
SG.AC-19	Control System Access Restrictions			2.15.28	External Access Protections	
SG.AC-20	Publicly Accessible Content					
SG.AC-21	Passwords			2.15.16	Passwords	CIP 007-2 (R5.3)
Awareness and Training (SG.AT)						

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
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**
SG.AT-1	Awareness and Training Policy and Procedures	AT-1	Security Awareness and Training Policy and Procedures	2.11.1	Security Awareness Training Policy and Procedures	CIP 004-2 (R1, R2)
SG.AT-2	Security Awareness	AT-2	Security Awareness	2.11.2	Security Awareness	CIP 004-2 (R1)
SG.AT-3	Security Training	AT-3	Security Training	2.11.3	Security Training	CIP 004-2 (R2)
SG.AT-4	Security Awareness and Training Records	AT-4	Security Training Records	2.11.4	Security Training Records	CIP 004-2 (R2.3)
SG.AT-5	Contact with Security Groups and Associations	AT-5	Contact with Security Groups and Associations	2.11.5	Contact with Security Groups and Associations	
SG.AT-6	Security Responsibility Training			2.11.6	Security Responsibility Training	
SG.AT-7	Planning Process Training			2.7.5	Planning Process Training	CIP 004-2 (R2)
Audit and Accountability (SG.AU)						
SG.AU-1	Audit and Accountability	AU-1	Audit and Accountability Policy and Procedures	2.16.1	Audit and Accountability Process and Procedures	CIP 003-2 (R1, R1.1, R1.3)
SG.AU-2	Auditable Events	AU-2	Auditable Events	2.16.2	Auditable Events	CIP 005-2 (R1, R1.1, R1.3) CIP 007-2 (R5.1.2, R5.2.3, R6.1, R6.3)
		AU-13	Monitoring for Information Disclosure			
SG.AU-3	Content of Audit Records	AU-3	Content of Audit Records	2.16.3	Content of Audit Records	CIP 007-3 (R5.1.2)
SG.AU-4	Audit Storage Capacity	AU-4	Audit Storage Capacity	2.16.4	Audit Storage	

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

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) May 2009
SG.AU-5	Response to Audit Processing Failures	AU-5	Response to Audit Processing Failures	2.16.5	Response to Audit Processing Failures	
SG.AU-6	Audit Monitoring, Analysis, and Reporting	AU-6	Audit Monitoring, Analysis, and Reporting	2.16.6	Audit Monitoring, Process, and Reporting	CIP 007-2 (R5.1.2) CIP 007-2 (R6.5)
SG.AU-7	Audit Reduction and Report Generation	AU-7	Audit Reduction and Report Generation	2.16.7	Audit Reduction and Report Generation	
SG.AU-8	Time Stamps	AU-8	Time Stamps	2.16.8	Time Stamps	
SG.AU-9	Protection of Audit Information	AU-9	Protection of Audit Information	2.16.9	Protection of Audit Information	CIP 003-2 (R4)
SG.AU-10	Audit Record Retention	AU-11	Audit Record Retention	2.16.10	Audit Record Retention	CIP 005-2 (R5.3) CIP 007-2 (R5.1.2, R6.4) CIP 008-2 (R2)
SG.AU-11	Conduct and Frequency of Audits	AU-1	Audit and Accountability Policy and Procedures	2.16.11	Conduct and Frequency of Audits	
SG.AU-12	Auditor Qualification			2.16.12	Auditor Qualification	
SG.AU-13	Audit Tools	AU-7	Audit Reduction and Report Generation	2.16.13	Audit Tools	
SG.AU-14	Security Policy Compliance	CA-1	Security Assessment and Authorization Policies and Procedures	2.16.14	Security Policy Compliance	
SG.AU-15	Audit Generation	AU-12	Audit Generation	2.16.15	Audit Generation	
SG.AU-16	Non-Repudiation	AU-10	Non-Repudiation	2.16.16	Non-Repudiation	
Security Assessment and Authorization (SG.CA)						

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
SG.CA-1	Security Assessment and Authorization Policy and Procedures	CA-1	Security Assessment and Authorization Policies and Procedures	2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures	
				2.17.1	Monitoring and Reviewing Control System Security management Policy and Procedures	
SG.CA-2	Security Assessments	CA-2	Security Assessments	2.17.3	Monitoring of Security Policy	
SG.CA-3	Continuous Improvement			2.17.2	Continuous Improvement	
				2.17.4	Best Practices	
SG.CA-4	Information System Connections	CA-3	Information System Connection	2.18.5	Control System Connections	CIP 005-2 (R2)
SG.CA-5	Security Authorization to Operate	CA-6	Security Authorization	2.17.5	Security Accreditation	
		PM-10	Security Authorization Process			
SG.CA-6	Continuous Monitoring	CA-7	Continuous Monitoring	2.18.7	Continuous Monitoring	
Configuration Management (SG.CM)						
SG.CM-1	Configuration Management Policy and Procedures	CM-1	Configuration Management Policy and Procedures	2.6.1	Configuration Management Policy and Procedures	CIP 003-2 (R6)
SG.CM-2	Baseline Configuration	CM-2	Baseline Configuration	2.6.2	Baseline Configuration	CIP 007-2 (R9)
SG.CM-3	Configuration Change Control	CM-3	Configuration Change Control	2.6.3	Configuration Change Control	CIP 003-2 (R6)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
		SA-10	Developer Configuration Management			
SG.CM-4	Monitoring Configuration Changes	CM-4 SA-10	Security Impact Analysis Developer Configuration Management	2.6.4	Monitoring Configuration Changes	CIP 003-2 (R6)
SG.CM-5	Access Restrictions for Configuration Change	CM-5	Access Restrictions for Change	2.6.5	Access Restrictions for Configuration Change	CIP 003-2 (R6)
SG.CM-6	Configuration Settings	CM-6	Configuration Settings	2.6.6	Configuration Settings	CIP 003-2 (R6) CIP 005 (R2.2)
SG.CM-7	Configuration for Least Functionality	CM-7	Least Functionality	2.6.7	Configuration for Least Functionality	
SG.CM-8	Component Inventory	CM-8	Information System Component Inventory	2.6.8	Configuration Assets	
SG.CM-9	Addition, Removal, and Disposal of Equipment	MP-6	Media Sanitization	2.6.9	Addition, Removal, and Disposition of Equipment	CIP 003-2 (R6)
SG.CM-10	Factory Default Settings Management			2.6.10	Factory Default Authentication Management	CIP 005-2 (R4.4)
SG.CM-11	Configuration Management Plan	CM-9	Configuration Management Plan			
Continuity of Operations (SG.CP)						
SG.CP-1	Continuity of Operations Policy and Procedures	CP-1	Contingency Planning Policy and Procedures			

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
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**
SG.CP-2	Continuity of Operations Plan	CP-1	Contingency Planning Policy and Procedures	2.12.2	Continuity of Operations Plan	CIP 008-2 (R1) CIP 009-2 (R1)
SG.CP-3	Continuity of Operations Roles and Responsibilities	CP-2	Contingency Plan	2.12.3	Continuity of Operations Roles and Responsibilities	CIP 009-2 (R1.1, R1.2)
SG.CP-4	Continuity of Operations Training					
SG.CP-5	Continuity of Operations Plan Testing	CP-4	Contingency Plan Testing and Exercises	2.12.5	Continuity of Operations Plan Testing	CIP 008-2 (R1.6) CIP 009-2 (R2, R5)
SG.CP-6	Continuity of Operations Plan Update			2.12.6	Continuity of Operations Plan Update	CIP 009-2 (R4, R5)
SG.CP-7	Alternate Storage Sites	CP-6	Alternate Storage Sites	2.12.13	Alternative Storage Sites	
SG.CP-8	Alternate Telecommunication Services	CP-8	Telecommunications Services	2.12.14	Alternate Command/Control Methods	
SG.CP-9	Alternate Control Center	CP-7 CP-8	Alternate Processing Site Telecommunications Services	2.12.15	Alternate Control Center	
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	CP-10	Information System Recovery and Reconstitution	2.12.17	Control System Recovery and Reconstitution	CIP 009-2 (R4)
SG.CP-11	Fail-Safe Response			2.12.18	Fail-Safe Response	
Identification and Authentication (SG.IA)						
SG.IA-1	Identification and Authentication Policy	IA-1	Identification and Authentication Policy and	2.15.2	Identification and Authentication	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
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**
	and Procedures		Procedures		Procedures and Policy	
SG.IA-2	Identifier Management	IA-4	Identifier Management	2.15.4	Identifier Management	
SG.IA-3	Authenticator Management	IA-5	Authenticator Management	2.15.5	Authenticator Management	CIP 007-2 (R5, R5.1, R5.2, R5.3)
SG.IA-4	User Identification and Authentication	IA-2	User Identification and Authentication	2.15.10	User Identification and Authentication	CIP 003-2 (R1, R1.1, R1.3)
SG.IA-5	Device Identification and Authentication	IA-3	Device Identification and Authentication	2.15.12	Device Authentication and Identification	
SG.IA-6	Authenticator Feedback	IA-6	Authenticator Feedback	2.15.13	Authenticator Feedback	
Information and Document Management (SG.ID)						
SG.ID-1	Information and Document Management Policy and Procedures			2.9.1	Information and Document Management Policy and Procedures	
SG.ID-2	Information and Document Retention			2.9.2	Information and Document Retention	CIP 006-2 (R7)
SG.ID-3	Information Handling	MP-1	Media Protection Policy and Procedures	2.9.3	Information Handling	CIP 003-2 (R4.1)
SG.ID-4	Information Exchange			2.9.5	Information Exchange	
SG.ID-5	Automated Labeling			2.9.11	Automated Labeling	
Incident Response (SG.IR)						
SG.IR-1	Incident Response Policy and Procedures	IR-1	Incident Response Policy and Procedures	2.12.1	Incident Response Policy and Procedures	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
SG.IR-2	Incident Response Roles and Responsibilities	IR-1	Incident Response Policy and Procedures	2.7.4	Roles and Responsibilities	CIP 008-2 (Rr1.2) CIP 009-2 (R1.2)
SG.IR-3	Incident Response Training	IR-2	Incident Response Training	2.12.4	Incident Response Training	
SG.IR-4	Incident Response Testing and Exercises	IR-3	Incident Response Testing and Exercises			
SG.IR-5	Incident Handling	IR-4	Incident Handling	2.12.7	Incident Handling	
SG.IR-6	Incident Monitoring	IR-5	Incident Monitoring	2.12.8	Incident Monitoring	
SG.IR-7	Incident Reporting	IR-6	Incident Reporting	2.12.9	Incident Reporting	
SG.IR-8	Incident Response Investigation and Analysis	PE-6	Monitoring Physical Access	2.12.11	Incident Response Investigation and Analysis	CIP 008-2 (R1, R1.2-R1.5)
SG.IR-9	Corrective Action			2.12.12	Corrective Action	CIP 008-2 (R1.4) CIP 009-2 (R3)
SG.IR-10	Smart Grid Information System Backup	CP-9	Information System Backup	2.12.16	Control System Backup	
SG.IR-11	Coordination of Emergency Response			2.2.4	Coordination of Threat Mitigation	CIP 008-2 (R1.3)
Smart Grid Information System Development and Maintenance (SG.MA)						
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	MA-1	System Maintenance Policy and Procedures	2.10.1	System Maintenance Policy and Procedures	
SG.MA-2	Legacy Smart Grid Information System Updates			2.10.2	Legacy System Upgrades	

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

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) May 2009
SG.MA-3	Smart Grid Information System Maintenance	PL-6	Security-Related Activity Planning	2.10.5	Unplanned System Maintenance	
		MA-2	Controlled Maintenance	2.10.6	Periodic System Maintenance	
SG.MA-4	Maintenance Tools	MA-3	Maintenance Tools	2.10.7	Maintenance Tools	
SG.MA-5	Maintenance Personnel	MA-5	Maintenance Personnel	2.10.8	Maintenance Personnel	
SG.MA-6	Remote Maintenance	MA-4	Non-Local Maintenance	2.10.9	Remote Maintenance	
SG.MA-7	Timely Maintenance	MA-6	Timely Maintenance	2.10.10	Timely Maintenance	CIP 009-2 (R4)
Media Protection (SG.MP)						
SG.MP-1	Media Protection Policy and Procedures	MP-1	Media Protection Policy and Procedures	2.13.1	Media Protection and Procedures	
SG.MP-2	Media Sensitivity Level	RA-2	Security Categorization	2.13.3	Media Classification	CIP 003-2 (R4, R4.2)
				2.9.4	Information Classification	
SG.MP-3	Media Marketing	MP-3	Media Marketing	2.13.4	Media Labeling	
				2.9.10	Automated Marking	
SG.MP-4	Media Storage	MP-4	Media Storage	2.13.5	Media Storage	
SG.MP-5	Media Transport	MP-5	Media Transport	2.13.6	Media Transport	
SG.MP-6	Media Sanitization and Disposal	MP-6	Media Sanitization	2.13.7	Media Sanitization and Storage	CIP 007-2 (R7, R7.1, R7.2, R7.3)
Physical and Environmental Security (SG.PE)						
SG.PE-1	Physical and Environmental Security Policy and Procedures	PE-1	Physical and Environmental Protection Policy and Procedures	2.4.1	Physical and Environmental Security Policies and Procedures	CIP 006-2 (R1, R2)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
SG.PE-2	Physical Access Authorizations	PE-2	Physical Access Authorizations	2.4.2	Physical Access Authorizations	CIP 004-2 (R4)
SG.PE-3	Physical Access	PE-3	Physical Access Control	2.4.3	Physical Access Control	CIP 006-2 (R2)
		PE-4	Access Control for Transmission Medium			
		PE-5	Access Control for Output Devices			
SG.PE-4	Monitoring Physical Access	PE-6	Monitoring Physical Access	2.4.4	Monitoring Physical Access	CIP 006-2 (R5)
SG.PE-5	Visitor Control	PE-7	Visitor Control	2.4.5	Visitor Control	CIP 006-2 (R1.4)
SG.PE-6	Visitor Records	PE-8	Access Records	2.4.6	Visitor Records	CIP 006-2 (R1.4, R6)
SG.PE-7	Physical Access Log Retention			2.4.7	Physical Access Log Retention	CIP 006-2 (R7)
SG.PE-8	Emergency Shutoff Protection	PE-10	Emergency Shutoff	2.4.8	Emergency Shutoff	
SG.PE-9	Emergency Power	PE-11	Emergency Power	2.4.9	Emergency Power	
SG.PE-10	Delivery and Removal	PE-16	Delivery and Removal	2.4.14	Delivery and Removal	
SG.PE-11	Alternate Work Site	PE-17	Alternate Work Site	2.4.15	Alternate Work Site	
SG.PE-12	Location of Smart Grid Information System Assets	PE-18	Location of Information System Components	2.4.18	Location of Control System Assets	
Planning (SG.PL)						
SG.PL-1	Strategic Planning Policy and Procedures	PL-1	Security Planning and Procedures	2.7.1	Strategic Planning Policy and Procedures	

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

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) May 2009
SG.PL-2	Smart Grid Information System Security Plan	PL-2	System Security Plan	2.7.2	Control System Security Plan	
SG.PL-3	Rules of Behavior	PL-4	Rules of Behavior	2.7.11	Rules of Behavior	
SG.PL-4	Privacy Impact Assessment	PL-5	Privacy Impact Assessment			
SG.PL-5	Security-Related Activity Planning	PL-6	Security-Related Activity Planning	2.7.12	Security-Related Activity Planning	CIP 002-2 (R1)
Security Program Management (SG.PM)						
SG.PM-1	Security Policy and Procedures	AC-1	Access Control Policy and Procedures	2.1.1	Security Policies and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)
SG.PM-2	Security Program Plan	PM-1	Information Security Program Plan			
SG.PM-3	Senior Management Authority	PM-2	Senior Information Security Officer			
SG.PM-4	Security Architecture	PM-7	Enterprise Architecture			
SG.PM-5	Risk Management Strategy	PM-9	Risk Management Strategy			
SG.PM-6	Security Authorization to Operate Process	PM-10	Security Authorization Process			
SG.PM-7	Mission/Business Process Definition	PM-11	Mission/Business Process Definition			
SG.PM-8	Management Accountability	PM-1	Information Security Program Plan	2.2.2	Management Accountability	CIP 003-2 (R2, R3)
Personnel Security (SG.PS)						

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
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**
SG.PS-1	Personnel Security Policy and Procedures	PS-1	Personnel Security Policy and Procedures	2.3.1	Personnel Security Policies and Procedures	CIP 004-2 (R3)
SG.PS-2	Position Categorization	PS-2	Position Categorization	2.3.2	Position Categorization	CIP 004-2 (R3)
SG.PS-3	Personnel Screening	PS-3	Personnel Screening	2.3.3	Personnel Screening	CIP 004-2 (R3)
SG.PS-4	Personnel Termination	PS-4	Personnel Termination	2.3.4	Personnel Termination	CIP 004-2 (R4.2) CIP 004-2 (R5.2.3)
SG.PS-5	Personnel Transfer	PS-5	Personnel Transfer	2.3.5	Personnel Transfer	CIP 004-2 (R4.1, R4.2)
SG.PS-6	Access Agreements	PS-6	Access Agreements	2.3.6	Access Agreements	
SG.PS-7	Contractor and Third-Party Personnel Security	PS-7	Third-Party Personnel Security	2.3.7	Third-Party Security Agreements	CIP 004-2 (R3.3)
SG.PS-8	Personnel Accountability	PS-8	Personnel Sanctions	2.3.8	Personnel Accountability	
SG.PS-9	Personnel Roles			2.3.9	Personnel Roles	
Risk Management and Assessment (SG.RA)						
SG.RA-1	Risk Assessment Policy and Procedures	RA-1	Risk Assessment Policy and Procedures	2.18.1	Risk Assessment Policy and Procedures	CIP 002-2 (R1, R1.1, R1.2, R4) CIP 003-2 (R1, R4.2)
SG.RA-2	Risk Management Plan	PM-9	Risk Management Strategy	2.18.2	Risk Management Plan	CIP 003-2 (R4, R4.1, R4.2)
SG.RA-3	Security Impact Level	RA-2	Security Categorization	2.18.8	Security Categorization	
SG.RA-4	Risk Assessment	RA-3	Risk Assessment	2.18.9	Risk Assessment	CIP 002-2 (R1.2)
SG.RA-5	Risk Assessment Update	RA-3	Risk Assessment	2.18.10	Risk Assessment Update	CIP 002-2 (R4)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
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**
SG.RA-6	Vulnerability Assessment and Awareness	RA-5	Vulnerability Scanning	2.18.11	Vulnerability Assessment and Awareness	CIP 005-2 (R4, R4.2, R4.3, R4.4) CIP 007-2 (R8)
Smart Grid Information System and Services Acquisition (SG.SA)						
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	SA-1	System and Services Acquisition Policy and Procedures	2.5.1	System and Services Acquisition Policy and Procedures	
SG.SA-2	Security Policies for Contractors and Third Parties			2.2.5	Security Policies for Third Parties	
				2.2.6	Termination of Third-Party Access	
SG.SA-3	Life-Cycle Support	SA-3	Life-Cycle Support	2.5.3	Life-Cycle Support	
SG.SA-4	Acquisitions	SA-4	Acquisitions	2.5.4	Acquisitions	
SG.SA-5	Smart Grid Information System Documentation	SA-5	Information System Documentation	2.5.5	Control System Documentation	
SG.SA-6	Software License Usage Restrictions	SA-6	Software Usage Restrictions	2.5.6	Software License Usage Restrictions	
SG.SA-7	User-Installed Software	SA-7	User-Installed Software	2.5.7	User-installed Software	
SG.SA-8	Security Engineering Principles	SA-8 SA-13	Security Engineering Principles	2.5.8	Security Engineering Principals	
			Trustworthiness			
SG.SA-9	Developer Configuration Management	SA-10	Developer Configuration Management	2.5.10	Vendor Configuration Management	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
SG.SA-10	Developer Security Testing	SA-11	Developer Security Testing	2.5.11	Vendor Security Testing	
SG.SA-11	Supply Chain Protection	SA-12	Supply Chain Protection	2.5.12	Vendor Life-cycle Practices	
Smart Grid Information System and Communication Protection (SG.SC)						
SG.SC-1	System and Communication Protection Policy and Procedures	SC-1	System and Communication Protection Policy and Procedures	2.8.1	System and Communication Protection Policy and Procedures	CIP 003-2 (R1, R1.1, R1.3)
SG.SC-2	Communications Partitioning			2.8.2	Management Port Partitioning	
SG.SC-3	Security Function Isolation	SC-3	Security Function Isolation	2.8.3	Security Function Isolation	
SG.SC-4	Information Remnants	SC-4	Information in Shared Resources	2.8.4	Information Remnants	
SG.SC-5	Denial-of-Service Protection	SC-5	Denial-of-Service Protection	2.8.5	Denial-of-Service Protection	
SG.SC-6	Resource Priority	SC-6	Resource Priority	2.8.6	Resource Priority	
SG.SC-7	Boundary Protection	SC-7	Boundary Protection	2.8.7	Boundary Protection	CIP 005-2 (R1, R1.1, R1.2, R1.3, R1.4, R1.6, R2, R2.1-R2.4, R5, R5.1)
SG.SC-8	Communication Integrity	SC-8	Transmission Integrity	2.8.8	Communication Integrity	
SG.SC-9	Communication Confidentiality	SC-9	Transmission Confidentiality	2.8.9	Communication Confidentially	
SG.SC-10	Trusted Path	SC-11	Trusted Path	2.8.10	Trusted Path	
SG.SC-11	Cryptographic Key Establishment and Management	SC-12	Cryptographic Key Establishment and Management	2.8.11	Cryptographic Key Establishment and Management	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
SG.SC-12	Use of Validated Cryptography	SC-13	Use of Cryptography	2.8.12	Use of Validated Cryptography	
SG.SC-13	Collaborative Computing	SC-15	Collaborative Computing Devices	2.8.13	Collaborative Computing	
SG.SC-14	Transmission of Security Parameters	SC-16	Transmission of Security Attributes	2.8.14	Transmission of Security Parameters	
SG.SC-15	Public Key Infrastructure Certificates	SC-17	Public Key Infrastructure Certificates	2.8.15	Public Key Infrastructure Certificates	
SG.SC-16	Mobile Code	SC-18	Mobile Code	2.8.16	Mobile Code	
SG.SC-17	Voice-Over Internet Protocol	SC-19	Voice Over Internet Protocol	2.8.17	Voice-over-Internet Protocol	
SG.SC-18	System Connections	CA-3	Information System Connections	2.8.18	System Connections	CIP 005-2 (R2, R2.2-R2.4)
SG.SC-19	Security Roles	SA-9	External Information System Services	2.8.19	Security Roles	CIP 003-2 (R5)
SG.SC-20	Message Authenticity	SC-8	Transmission Integrity	2.8.20	Message Authenticity	
SG.SC-21	Secure Name/Address Resolution Service	SC-20	Secure Name/Address Resolution Service (Authoritative Source)	2.8.22	Secure Name/Address Resolution Service (Authoritative Source)	
SG.SC-22	Fail in Known State	SC-24	Fail in Known State	2.8.24	Fail in Know State	
SG.SC-23	Thin Nodes	SC-25	Thin Nodes	2.8.25	Thin Nodes	
SG.SC-24	Honeypots	SC-26	Honeypots	2.8.26	Honeypots	
SG.SC-25	Operating System-Independent Applications	SC-27	Operating System-Independent Applications	2.8.27	Operating System-Independent Applications	
SG.SC-26	Confidentiality of Information at Rest	SC-28	Confidentiality of Information at Rest	2.8.28	Confidentiality of Information at Rest	
SG.SC-27	Heterogeneity	SC-29	Heterogeneity	2.8.29	Heterogeneity	

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)		Light Gray = Common Technical Requirement				
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**
SG.SC-28	Virtualization Technique	SC-30	Virtualization Technique	2.8.30	Virtualization Techniques	
SG.SC-29	Application Partitioning			2.8.32	Application Partitioning	
SG.SC-30	Information System Partitioning	SC-32	Information Systems Partitioning			
Smart Grid Information System and Information Integrity (SG.SI)						
SG.SI-1	System and Information Integrity Policy and Procedures	SI-1	System and Information Integrity Policy and Procedures	2.14.1	System and Information Integrity Policy and Procedures	
SG.SI-2	Flaw Remediation	SI-2	Flaw Remediation	2.14.2	Flaw Remediation	CIP 007-2 (R3, R3.1, R3.2)
SG.SI-3	Malicious Code and Spam Protection	SI-3	Malicious Code Protection	2.14.3	Malicious Code Protection	CIP 007-2 (R4, R4.1, R4.2)
		SI-8	Spam Protection	2.14.8	Spam Protection	CIP 007-2 (R4)
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	SI-4	Information System Monitoring	2.14.4	System Monitoring Tools and Techniques	CIP 007-2 (R6)
SG.SI-5	Security Alerts and Advisories	SI-5	Security Alerts, Advisories, and Directives	2.14.5	Security Alerts and Advisories	
SG.SI-6	Security Functionality Verification	SI-6	Security Functionality Verification	2.14.6	Security Functionality Verification	CIP 007-2 (R1)
SG.SI-7	Software and Information Integrity	SI-7	Software and Information Integrity	2.14.7	Software and Information Integrity	
SG.SI-8	Information Input Validation	SI-10	Information Input Validation	2.14.9	Information Input Restrictions	CIP 003-2 (R5) CIP 007-2 (R, R5.1, R5.2)

Dark Gray = Unique Technical Requirement White = Common Governance, Risk and Compliance (GRC)			Light Gray = Common Technical Requirement			
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**
				2.14.10	Information Input Accuracy, Completeness, Validity and Authenticity	
SG.SI-9	Error Handling	SI-11	Error Handling	2.14.11	Error Handling	