EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security Risk Management in Practice

Comparative Analyses Tables

3002004712

Cyber Security Risk Management in Practice

Comparative Analyses Tables

3002004712

Technical Update, December 2014

EPRI Project Manager

A. Lee

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT.

THIS REPORT WAS PREPARED AS AN ACCOUNT OF WORK SPONSORED BY AN AGENCY OF THE UNITED STATES GOVERNMENT. NEITHER THE UNITED STATES GOVERNMENT NOR ANY AGENCY THEREOF, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OR IMPLIED, OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS. REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF. THE VIEWS AND OPINIONS OF AUTHORS EXPRESSED HEREIN DO NOT NECESSARILY STATE OR REFLECT THOSE OF THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF.

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2014 Electric Power Research Institute, Inc. All rights reserved.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigator
A. Lee

This report describes research sponsored by EPRI.

The following organization and individuals participated in the development of this technical update:

Maurice Martin, Craig Miller, George Walker: National Rural Electric Cooperative Association (NRECA)

In addition, several individuals provided feedback and recommendations on the development of the document.

The dedication and commitment of all the participants was significant and the technical content could not have been developed without their contributions.

Some of the material included in this technical update is based on several documents, for example, the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, September 2014; the U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1*, February 2014, and the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, February 2014. The authors acknowledge the dedication and technical expertise of all the individuals who participated in the development of these documents.

This publication is a corporate document that should be cited in the literature in the following manner:

Cyber Security Risk Management in Practice: Comparative Analyses Tables. EPRI, Palo Alto, CA: 2014. 3002004712.

ABSTRACT

Utilities are assessing various federal guidelines that are applicable to cyber security for the electric sector—a significant task requiring all new guidance. This report is a companion document to EPRI technical update 3002003333, *Risk Management in Practice—A Guide for the Electric Sector*, and EPRI technical update 3002003332, *Security Posture Using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. The focus of this technical update is to provide guidance on the various cyber security regulations, guidelines, and specifications that may be applicable to the electric sector. This update is not intended to provide new guidance but rather to present information on how to navigate and relate the diverse existing guidance that is applicable to the electric sector. To this end, several additional comparative analyses tables referenced in the other two documents will serve as a roadmap for utilities to use in understanding and applying the cyber security guidance. Information in the various tables will also help utilities implement their own cyber security programs and perform cyber security risk management activities, including risk and maturity assessments.

Keywords
Cyber security
Cyber security regulations
Failure scenarios
Maturity assessments
Risk management
Risk assessments

This publication is a corporate document that should be cited in the literature in the following manner:

Cyber Security Risk Management in Practice: Comparative Analyses Tables. EPRI, Palo Alto, CA: 2014. 3002004712.

CONTENTS

LIST OF TABLES

1
COMPARATIVE ANALYSES TABLES

Several comparative analyses tables are referenced in the EPRI technical updates 3002004712, 3002003332, Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and 3002003333, Risk Management in Practice - A Guide for the Electric Sector provide guidance. These comparative analyses tables are included in this document.

1.1 NISTIR 7628, NIST SP 800-53, and the NIST CSF

Table 1-1 below is a comparative analysis between the NISTIR 7628, the NIST SP 800-53 rev 4, and the NIST CSF. In the table, comparable NISTIR 7628 requirements and NIST SP 800-53 requirements are listed next to each other. For example, SG.CM-2 and CM-2 correspond and are listed next to each other. Because SP 800-53 has been revised since the publication of the NISTIR 7628, some of the corresponding controls do not have the same reference number, for example, SG.PM-4 (NISTIR 7628) and PM-7 (NIST SP800-53, Rev 4). Also, if there are additional controls from either the NISTIR 7628 or SP 800-53 Rev 4, they are listed in the appropriate cell without a corresponding control in the other column.

Table 1-1
Comparative Analysis of the NISTIR 7628, the NIST SP 800-53 Rev 4, and the NIST CSF.

[The following information is extracted from the NIST CSF, the NISTIR 7628, and NIST SP 800-53, Rev 4.]

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
IDENTIFY (ID)	**Asset Management (AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	SG.CM-2 SG.CM-8	CM-2 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	SG.CM-2 SG.CM-8	CM-2 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	SG.AC-5 SG.CA-4 SG.PM-4	AC-4 CA-3 PM-7 CA-9 PL-8
		ID.AM-4: External information systems are catalogued	SG.AC-18	AC-20

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	SG.CP-2 SG.RA-3 SG.SC-6	CP-2 RA-2 SG.SC-6 SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	SG.CP-3 SG.PL-3 SG.PS-9 SG.SC-19	CP-2 PL-4 PS-7
	Business Environment (BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated		
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated		
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	SG.PM-7	PM-11 SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	SG.CP-9 SG.SA-11	CP-7 SA-12 SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	SG.CP-2 SG.CP-10	CP-2 CP-10

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
	Governance (GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	All -1 Requirements	-1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	SG.PS-9 SG.SC-19	PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	All -1 Requirements	-1 controls from all families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	SG.PM-5	PM-9
	Risk Assessment (RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	SG.CA-2 SG.CA-6 SG.RA-6 SG.SA-10 SG.SI-2 SG.SI-5	CA-2 CA-7 RA-5 SA-11 SI-2 SI-5 CA-8

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	SG.AT-5 SG.SI-5	PM-15 SI-5 PM-16
		ID.RA-3: Threats, both internal and external, are identified and documented	SG.RA-4 SG.SI-5	RA-3 SI-5 PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	SG.RA-3 SG.RA-4 SG.PM-5 SG.PM-7	RA-2 RA-3 PM-9 PM-11 SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	SG.RA-3 SG.RA-4	RA-2 RA-3 PM-16
		ID.RA-6: Risk responses are identified and prioritized	SG.PM-5	PM-9 PM-4
	Risk Management Strategy (RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	SG.PM-5	PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	SG.PM-5 SG.RA-2	PM-9 PM-9

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
		ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	SG.PM-5 SG.PM-7	PM-9 PM-11 PM-8 SA-14
PROTECT (PR)	**Access Control (AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	SG.AC-3 SG.IA-2 IA-3 SG.IA-4 SG.IA-5 SG.AC-19 SG.AC-21	AC-2 IA-4 IA-5 IA-2 IA-3 IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	SG.PE-2 SG.PE-3	PE-2 PE-3, PE-4, PE-5
		PR.AC-3: Remote access is managed	SG.AC-2 SG.AC-13 SG.AC-15	AC-17 AC-17

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	SG.AC-6 SG.AC-7	AC-5 AC-6
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	SG.AC-5 SG.SC-7 SG.AC-19	AC-4 SC-7
	Awareness and Training (AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	SG.AT-2 SG.AT-3 SG.AT-7	AT-2 AT-3 PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	SG.AT-3 SG.IR-3 SG.PS-9 SG.CP-4 SG.SC-19	SG.AT-3 SG.IR-2 PS-7 PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	SG.PS-9	PS-7 SA-9

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
		PR.AT-4: Senior executives understand roles & responsibilities	SG.AT-3 SG.PM-8 SG.PS-9	AT-3 PS-7 PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	SG.AT-3 SG.PS-9	AT-3 PS-7 PM-13
	Data Security (DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	SG.SC-26	SC-28
		PR.DS-2: Data-in-transit is protected	SG.SC-8 SG.SC-9	SC-8 SC-9

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	SG.CM-8 SG.CM-9 SG.MP-6 SG.PE-10	CM-8 MP-6 MP-6 PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	SG.SC-5	SC-5
		PR.DS-5: Protections against data leaks are implemented	SG.AC-5 SG.AC-6 SG.AC-7 SG.SC-7 SG.SC-9 SG.SC-12	AC-4 AC-5 AC-6 SC-7 SC-9 SC-13 PE-19 SC-31
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SG.SI-7	SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	SG.CM-2	CM-2

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
	Information Protection Processes and Procedures (IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	SG.CM-2 SG.CM-6 SG.SA-9	CM-2 CM-6 SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	SG.SA-3 SG.SA-8 SG.SA-9 SG.SA-10	SA-3 SA-8 SA-10 SA-11 SA-15, SA-17
		PR.IP-3: Configuration change control processes are in place	SG.CM-3 SG.CM-4 SG.CM-5 SG.CM-6 SG.SA-9 SG.CM-10	CM-3 CM-4 CM-5 CM-6 SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	SG.CP-5 SG.IR-10	CP-4 CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	SG.PE-1 SG.PE-8 SG.PE-9 SG.PE-12	PE-1 PE-10 PE-11 PE-18 PE-12, PE-13, PE-14, PE-15,
		PR.IP-6: Data is destroyed according to policy	SG.MP-6	MP-6
		PR.IP-7: Protection processes are continuously improved	SG.CA-2 SG.CA-6 SG.PL-2 SG.CA-3	CA-2 CA-7 PL-2 PM-6

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	SG.AT-5	AT-5 AC-21
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	SC.CP-2 SG.CP-3 SG.CP-6 SG.IR-1 SG.IR-2 SG.IR-11	CP-2 CP-2 CP-2 IR-1 IR-8
		PR.IP-10: Response and recovery plans are tested	SG.CP-5 SG.IR-4	CP-4 IR-3
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	SG.PS-1 SG.PS-2 SG.PS-3 SG.PS-4 SG.PS-5 SG.PS-7 SG.PS-8 SG.PS-9	PS-1 PS-2 PS-3 PS-4 PS-5 PS-7 PS-8 PS-7
		PR.IP-12: A vulnerability management plan is developed and implemented	SG.RA-4 SG.RA-5 SG.RA-6 SG.SI-2	RA-3 RA-3 RA-5 SI-2
	Maintenance (MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	SG.MA-3 SG.MA-4 SG.MA-5 SG.MA-7	MA-2 MA-3 MA-5 MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	SG.MA-6	MA-4

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
	Protective Technology (PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	SG.AU-1 SG.AU-2 SG.AU-3 SG.AU-6 SG.AU-7 SG.AU-15	AU-1 AU-2 AU-3 AU-6 AU-7 AU-12
		PR.PT-2: Removable media is protected and its use restricted according to policy	SG.AC-17 SG.MP-4 SG.MP-5	AC-19 MP-4 MP-5 MP-2, MP-7
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	SG.AC-3 SG.AC-4 SG.CM-7	AC-2 AC-3 CM-7
		PR.PT-4: Communications and control networks are protected	SG.SC-7 SG.SC-18	SC-7 CA-3
DETECT (DE)	**Anomalies and Events (AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	SG.AU-6 SG.CA-6	AU-6 CA-7
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	SG.AU-6 SG.IR-5	AU-6 IR-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	SG.AU-6 SG.IR-5 SG.IR-6	AU-6 IR-4 IR-5
		DE.AE-4: Impact of events is determined	SG.IR-5	IR-4
		DE.AE-5: Incident alert thresholds are established	SG.SI-4	SI-4

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
	Security Continuous Monitoring (CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	SG.CA-6 SG.SC-7 SG.SI-4	CA-7 SC-7 SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	SG.PE-4	PE-6
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	SG.PS-1	PS-1 AU-13
		DE.CM-4: Malicious code is detected	SG.SI-3	SI-3
		DE.CM-5: Unauthorized mobile code is detected	SG.SC-16	SC-18 SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	SG.PS-7 SG.SI-4	PS-7 SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	SG.AC-15 SG.AC-17 SG.CM-4 SG.PE-4 SG.SI-4 SG.AC-16	AC-17 AC-19 CM-4 PE-6 SI-4 PE-20
		DE.CM-8: Vulnerability scans are performed	SG.RA-6	RA-5
	Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	SG.SC-19	PM-14

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
	timely and adequate awareness of anomalous events.	**DE.DP-2:** Detection activities comply with all applicable requirements	SG.CA-6	CA-7 PM-14
		DE.DP-3: Detection processes are tested	SG.SI-4	SI-4 PM-14
		DE.DP-4: Event detection information is communicated to appropriate parties	SG.AU-6 SG.IR-7	AU-6 IR-6
		DE.DP-5: Detection processes are continuously improved	SG.RA-6 SG.CA-3	RA-5 PM-14
RESPOND (RS)	**Response Planning (RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	SG.CP-2 SG.CP-10	CP-2 CP-10 IR-8
	Communications (CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	SG.CP-3 SG.IR-2 SG.IR-11	CP-2 IR-1 IR-8
		RS.CO-2: Events are reported consistent with established criteria	SG.IR-7	IR-6 IR-8
		RS.CO-3: Information is shared consistent with response plans	SG.CP-2 SG.IR-11	CP-2 IR-8

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	SG.CP-2 SG.IR-11	CP-2 IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	SG.AT-5 SG.SI-5	AT-5 SI-5 PM-15
	Analysis (AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	SG.AU-6 SG.IR-8	AU-6
		RS.AN-2: The impact of the incident is understood	SG.IR-5	IR-4
		RS.AN-3: Forensics are performed	SG.IR-5 SG.IR-8	IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	SG.CP-2	CP-2 IR-8
	Mitigation (MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	SG.IR-5	IR-4
		RS.MI-2: Incidents are mitigated	SG.IR-5	IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	SG.RA-6	RA-5
	Improvements (IM): Organizational response activities are improved by incorporating lessons learned from	**RS.IM-1:** Response plans incorporate lessons learned	SG.CP-2 SG.IR-5 SG.IR-9	CP-2 IR-4 IR-8

NIST Cybersecurity Framework			NISTIR 7628 Requirements	NIST SP 800-53 Rev 4
Function	**Category**	**Subcategory**		
	current and previous detection/response activities.	**RS.IM-2:** Response strategies are updated	SG.CP-6 SG.IR-1 SG.IR-2 SG.IR-5	CP-2 IR-1 IR-1 IR-4 IR-8
RECOVER (RC)	**Recovery Planning (RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	SG.CP-2	CP-2 IR-8
	Improvements (IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	SG.CP-6	CP-2 IR-8
		RC.IM-2: Recovery strategies are updated	SG.CP-6 SG.IR-1	CP-2 IR-1 IR-8
	Communications (CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed		
		RC.CO-2: Reputation after an event is repaired		
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	SG.CP-2	CP-2

1.2 NEI 08-09, NRC RG 5.71, and the NISTIR 7628 Requirements

Table 1-2 below includes a comparative analysis of the NEI 08-09, NRC RG 5.71, and the NISTIR 7628 requirements. The following requirements from each nuclear document did not map to any of the NISTIR 7628 security requirements.

NEI 08-09:

Appendix D: 1.20, 1.21

Appendix E: 3.11, 9.5, 9.6, 10.1

RG 5.71:

B.1.20, B.1.21, C.3.11, C.10.6, C.10.5, C.10.7, C.11.1

Table 1-2
Comparative Analysis of NEI 08-09, NRC RG 5.71, and the NISTIR 7628

[The following information is extracted from the NISTIR 7628, NRC RG 5.71, and NEI 08-09.]

NISTIR 7628	NEI 08-09	NRC RG 5.71
Access Control (SG.AC)		
SG.AC-1: Access Control Policy and Procedures	D – 1.1	B.1.1
SG.AC-2: Remote Access Policy and Procedures	D – 1.1	
SG.AC-3: Account Management	D – 1.2, 1.11	B.1.2, B.1.11
SG.AC-4: Access Enforcement	D – 1.3	B.1.3
SG.AC-5: Information Flow Enforcement	D – 1.4	B.1.4
SG.AC-6: Separation of Duties	D – 1.5	B.1.5
SG.AC-7: Least Privilege	D – 1.6, 5.3	B.1.6, B.5.3

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.AC-8: Unsuccessful Login Attempts	D – 1.7	B.1.7
SG.AC-9: Smart Grid Information System Use Notification	D – 1.8	B.1.8
SG.AC-10: Previous Logon Notification	D – 1.9	B.1.9
SG.AC-11: Concurrent Session Control		
SG.AC-12: Session Lock	D – 1.10	B.1.10
SG.AC-13: Remote Session Termination		
SG.AC-14: Permitted Actions without Identification or Authentication	D – 1.12	B.1.12
SG.AC-15: Remote Access	E - 6	C.6
SG.AC-16: Wireless Access Restrictions	D – 1.17	B.1.17
SG.AC-17: Access Control for Portable and Mobile Devices	D – 1.2, 1.19	B.1.19, C.1.2
SG.AC-18: Use of External Information Control Systems	D – 1.22	B.1.22
SG.AC-19: Control System Access Restrictions		
SG.AC-20: Publicly Accessible Content	D – 1.23	B.1.23
SG.AC-21: Passwords	D – 4.3	B.4.3
Awareness and Training (SG.AT)		

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.AT-1: Awareness and Training Policy and Procedures		
SG.AT-2: Security Awareness	E – 9.1, 9.2	C.10.1, C.10.2
SG.AT-3: Security Training	E – 9.1, 9.3	C.10.1, C.10.3
SG.AT-4: Security Awareness and Training Records	E – 9.7	C.10.8
SG.AT-5: Contact with Security Groups and Associations	E – 9.8	C.10.9
SG.AT-6: Security Responsibility Training	E – 9.4	C.10.4
SG.AT-7: Planning Process Training		
Audit and Accountability (SG.AU)		
SG.AU-1: Audit and Accountability Policy and Procedures	D – 2.1	B.2.1
SG.AU-2: Auditable Events	D – 2.2	B.2.2
SG.AU-3: Content of Audit Records	D – 2.3	B.2.3
SG.AU-4: Audit Storage Capacity	D – 2.4	B.2.4
SG.AU-5: Response to Audit Processing Failures	D – 2.5	B.2.5
SG.AU-6: Audit Monitoring, Analysis, and Reporting	D – 2.6	B.2.6
SG.AU-7: Audit Reduction and Report Generation	D – 2.7	B.2.7

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.AU-8: Time Stamps	D – 2.8	B.2.8
SG.AU-9: Protection of Audit Information	D – 2.9	B.2.9
SG.AU-10: Audit Record Retention	D – 2.11	B.2.11
SG.AU-11: Conduct and Frequency of Audits		
SG.AU-12: Auditor Qualification Requirement		
SG.AU-13: Audit Tools	D – 2.9	B.2.9
SG.AU-14: Security Policy Compliance		
SG.AU-15: Audit Generation	D – 2.12	B.2.12
SG.AU-16: Non-Repudiation	D – 2.10	B.2.10
Security Assessment and Authorization (SG.CA)		
SG.CA-1: Security Assessment and Authorization Policy and Procedures		
SG.CA-2: Security Assessments		
SG.CA-3: Continuous Improvement		
SG.CA-4: Information System Connections	D – 1.18, E – 3.4	B.1.18
SG.CA-5: Security Authorization to Operate		
SG.CA-6: Continuous Monitoring		C.4, C.4.1

NISTIR 7628	NEI 08-09	NRC RG 5.71
Configuration Management (SG.CM)		
SG.CM-1: Configuration Management Policy and Procedures	E – 10.2	C.11.2
SG.CM-2: Baseline Configuration	D – 5.4, E – 10.3	B.5.4, C.11.3
SG.CM-3: Configuration Change Control	D – 5.1, E – 10.4, 11.6	B.5.1, C.4.2, C.11.4
SG.CM-4: Monitoring Configuration Changes	D – 5.3, E – 10.5	B.5.3, C.11.5
SG.CM-5: Access Restrictions for Configuration Change	E – 10.6	C.11.6
SG.CM-6: Configuration Settings	D – 1.18, E – 10.7	B.1.18, C.11.7
SG.CM-7: Configuration for Least Functionality	D – 1.16, 5.1, 5.4, E – 10.8	B.1.16, B.5.1, B.5.4, C.11.8
SG.CM-8: Component Inventory	E – 10.9	C,11,9
SG.CM-9: Addition, Removal, and Disposal of Equipment		
SG.CM-10: Factory Default Settings Management	D – 4.1, 4.7	B.4.1, B.4.7
SG.CM-11: Configuration Management Plan		
Continuity of Operations (SG.CP)		
SG.CP-1: Continuity of Operations Policy and Procedures		C.9.1

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.CP-2: Continuity of Operations Plan	E – 8.1	C.9.2
SG.CP-3: Continuity of Operations Roles and Responsibilities	E – 8.1	C.9.2
SG.CP-4: Continuity of Operations Training	E – 8.3	C.9.4
SG.CP-5: Continuity of Operations Plan Testing	E – 8.2	C.9.3
SG.CP-6: Continuity of Operations Plan Update		
SG.CP-7: Alternate Storage Sites	E – 8.4	C.9.5
SG.CP-8: Alternate Telecommunication Services		
SG.CP-9: Alternate Control Center		
SG.CP-10: Smart Grid Information System Recovery and Reconstitution	E – 8.6	C.9.7
SG.CP-11: Fail-Safe Response		
Identification and Authentication (SG.IA)		
SG.IA-1: Identification and Authentication Policy and Procedures	D – 4.1	B.4.1
SG.IA-2: Identifier Management	D – 4.6	B.4.6
SG.IA-3: Authenticator Management	D – 4.7	B.4.7
SG.IA-4: User Identification and Authentication	D – 4.2	B.4.2
SG.IA-5: Device Identification and Authentication	D – 4.5	B.4.5
SG.IA-6: Authenticator Feedback	D – 4.8	B.4.8

NISTIR 7628	NEI 08-09	NRC RG 5.71
Information and Document Management (SG.ID)		
SG.ID-1: Information and Document Management Policy and Procedures	D – 1.2	C.1.2
SG.ID-2: Information and Document Retention	E – 3.10	C.3.10
SG.ID-3: Information Handling	E – 3.10	C.3.10
SG.ID-4: Information Exchange		
SG.ID-5: Automated Labeling	D – 1.13, 1.14	B.1.13, B.1.14
Incident Response (SG.IR)		
SG.IR-1: Incident Response Policy and Procedures	E – 7.1	C.8.1
SG.IR-2: Incident Response Roles and Responsibilities	E – 7.1, 7.6	C.8.1, C.8.7
SG.IR-3: Incident Response Training	E – 7.2	C.8.2
SG.IR-4: Incident Response Testing and Exercises	E – 7.3	C.8.3
SG.IR-5: Incident Handling	E – 7.4	C.8, C.8.4
SG.IR-6: Incident Monitoring	E – 7.5	C.8.5
SG.IR-7: Incident Reporting		C.8.6
SG.IR-8: Incident Response Investigation and Analysis		
SG.IR-9: Corrective Action	E – 3.11, 12	C.13.3

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.IR-10: Smart Grid Information System Backup	E – 8.5	C.9.6
SG.IR-11: Coordination of Emergency Response		
Smart Grid Information System Development and Maintenance (SG.MA)		
SG.MA-1: Smart Grid Information System Maintenance Policy and Procedures	E – 4.1	C.4.1
SG.MA-2: Legacy Smart Grid Information System Updates		
SG.MA-3: Smart Grid Information System Maintenance		
SG.MA-4: Maintenance Tools	E – 4.2	C.4.2
SG.MA-5: Maintenance Personnel	E – 4.3	C.4.3
SG.MA-6: Remote Maintenance		
SG.MA-7: Timely Maintenance		
Media Protection (SG.MP)		
SG.MP-1: Media Protection Policy and Procedures	E – 1.1	C.1.1
SG.MP-2: Media Sensitivity Level		
SG.MP-3: Media Marking	D – 1.13, E – 1.3	B.1.13, C.1.3
SG.MP-4: Media Storage	E – 1.4	C.1.4
SG.MP-5: Media Transport	E – 1.5	C.1.5
SG.MP-6: Media Sanitization and Disposal	E – 1.6	C.1.6

NISTIR 7628	NEI 08-09	NRC RG 5.71
Physical and Environmental Security (SG.PE)		
SG.PE-1: Physical and Environmental Security Policy and Procedures	E – 5.1	C.5.1
SG.PE-2: Physical Access Authorizations	E – 5.4	C.5.4
SG.PE-3: Physical Access	D – 4.4, E – 5.4, 5.5	B.4.4, C.5.4, C.5.5
SG.PE-4: Monitoring Physical Access	D – 4.4, E – 5.6, 5.7, 5.8	B.4.4, C.5.6, C.5.7, C.5.8
SG.PE-5: Visitor Control	E – 5.2, 5.9	C.5.2
SG.PE-6: Visitor Records	E – 5.9	C.5.9
SG.PE-7: Physical Access Log Retention		
SG.PE-8: Emergency Shutoff Protection		
SG.PE-9: Emergency Power		
SG.PE-10: Delivery and Removal		
SG.PE-11: Alternate Work Site		
SG.PE-12: Location of Smart Grid Information System Assets		
Planning (SG.PL)		
SG.PL-1: Strategic Planning Policy and Procedures		
SG.PL-2: Smart Grid Information System Security Plan		

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.PL-3: Rules of Behavior		
SG.PL-4: Privacy Impact Assessment		
SG.PL-5: Security-Related Activity Planning		
Security Program Management (SG.PM)		
SG.PM-1: Security Policy and Procedures		
SG.PM-2: Security Program Plan		
SG.PM-3: Senior Management Authority		
SG.PM-4: Security Architecture		
SG.PM-5: Risk Management Strategy		
SG.PM-6: Security Authorization to Operate Process		
SG.PM-7: Mission/Business Process Definition		
SG.PM-8: Management Accountability		
Personnel Security (SG.PS)		
SG.PS-1: Personnel Security Policy and Procedures	E – 2.1	C.2.1
SG.PS-2: Position Categorization		
SG.PS-3: Personnel Screening	E – 5.2	C.5.2
SG.PS-4: Personnel Termination	E – 2.2	C.2.2
SG.PS-5: Personnel Transfer	E – 2.2	C.2.2
SG.PS-6: Access Agreements	E – 5.2	C.5.2

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.PS-7: Contractor and Third-Party Personnel Security	E – 5.2	C.5.2
SG.PS-8: Personnel Accountability		
SG.PS-9: Personnel Roles		C.10.10
Risk Management and Assessment (SG.RA)		
SG.RA-1: Risk Assessment Policy and Procedures	E - 12	C.13.1
SG.RA-2: Risk Management Plan		C.13.2
SG.RA-3: Security Impact Level		
SG.RA-4: Risk Assessment		
SG.RA-5: Risk Assessment Update	D – 5.5	B.5.5
SG.RA-6: Vulnerability Assessment and Awareness	E - 12	C.13.1
Smart Grid Information System and Services Acquisition (SG.SA)		
SG.SA-1: Smart Grid Information System and Services Acquisition Policy and Procedures	E – 11.1	C.12.1
SG.SA-2: Security Policies for Contractors and Third Parties		
SG.SA-3: Life-Cycle Support		
SG.SA-4: Acquisitions		
SG.SA-5: Smart Grid Information System Documentation		

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.SA-6: Software License Usage Restrictions		
SG.SA-7: User-Installed Software		
SG.SA-8: Security Engineering Principles	E – 11.3, 11.4, 11.6	C.8.8, C.12.3, C.12.4, C.12.6
SG.SA-9: Developer Configuration Management		
SG.SA-10: Developer Security Testing	E – 11.5	C.12.5
SG.SA-11: Supply Chain Protection	E – 11.2	C.12.2
Smart Grid Information System and Communication Protection (SG.SC)		
SG.SC-1: System and Communication Protection Policy and Procedures	D – 3.1	B.3.1
SG.SC-2: Communications Partitioning	D – 3.3	B.3.3
SG.SC-3: Security Function Isolation	D – 3.2	B.3.2
SG.SC-4: Information Remnants	D – 3.3	B.3.3
SG.SC-5: Denial-of-Service Protection	D – 3.4	B.3.4
SG.SC-6: Resource Priority	D – 3.5	B.3.5
SG.SC-7: Boundary Protection	E - 6	C.6, C.7
SG.SC-8: Communication Integrity	D – 3.6	B.3.6
SG.SC-9: Communication Confidentiality	D – 3.7	B.3.7
SG.SC-10: Trusted Path	D – 3.8	B.3.8
SG.SC-11: Cryptographic Key Establishment and Management	D – 3.9	B.3.9

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.SC-12: Use of Validated Cryptography	D – 1.15, 3.9, 4.9	B.1.15, B.3.10, B.4.9
SG.SC-13: Collaborative Computing	D – 3.10	B.3.11
SG.SC-14: Transmission of Security Parameters	D – 3.11	B.3.12
SG.SC-15: Public Key Infrastructure Certificates	D – 3.12	B.3.13
SG.SC-16: Mobile Code	D – 3.13	B.3.14
SG.SC-17: Voice-Over Internet Protocol		
SG.SC-18: System Connections		
SG.SC-19: Security Roles		
SG.SC-20: Message Authenticity	D – 3.17	B.3.18
SG.SC-21: Secure Name/Address Resolution Service	D – 3.14	B.3.15
SG.SC-22: Fail in Known State	D – 3.21	B.3.22
SG.SC-23: Thin Nodes	D – 3.18	B.3.19
SG.SC-24: Honeypots		
SG.SC-25: Operating System-Independent Applications		
SG.SC-26: Confidentiality of Information at Rest	D – 3.19	B.3.20
SG.SC-27: Heterogeneity	D – 3.20	B.3.21
SG.SC-28: Virtualization Technique		
SG.SC-29: Application Partitioning	D – 3.2	B.3.2
SG.SC-30: Information System Partitioning	D – 1.15	B.1.15
Smart Grid Information System and Information Integrity (SG.SI)		
SG.SI-1: System and Information Integrity Policy and Procedures	E – 3.1	C.3.1

NISTIR 7628	NEI 08-09	NRC RG 5.71
SG.SI-2: Flaw Remediation	D – 5.5, E – 3.2, 11.6	B.5.5, C.3.2, C.12.6
SG.SI-3: Malicious Code and Spam Protection	E – 3.3	C.3.3
SG.SI-4: Smart Grid Information System Monitoring Tools and Techniques	D – 5.2, E – 3.4	B.5.2, C.3.4
SG.SI-5: Security Alerts and Advisories	E – 3.5	C.3.5
SG.SI-6: Security Functionality Verification	E – 3.6	C.3.6
SG.SI-7: Software and Information Integrity	E – 3.7	C.3.7
SG.SI-8: Information Input Validation	E – 3.8	C.3.8
SG.SI-9: Error Handling	E – 3.9	C.3.9

1.3 NESCOR Failure Scenarios, Common Mitigations, and Common Vulnerabilities

Table 1-3 below allocates the NESCOR failure scenarios, the common mitigations, and the common vulnerabilities to the applicable ES-C2M2 domains, objectives, and practices. The table only includes the ES-C2M2 domains and practices that have allocated NESCOR components.

Table 1-3
NESCOR Failure Scenarios, Common Mitigations, and Common Vulnerabilities

[The following information is extracted from the ES-C2M2 and the NESCOR Failure Scenarios and Impact Analyses document.]

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
7.1 Risk Management				
3. Management Activities				
MIL2	a. Documented practices are followed for risk management activities	DER.2	Verify, verify network changes	
7.2 Asset, Change and Configuration Management				
				• Business logic vulnerability • Inadequate change and configuration management • Inadequate patch management process
1. Manage Asset Inventory				
MIL1	a. There is an inventory of OT and IT assets that are important to the delivery of the function	AMI.21	Track, track assets	
2. Manage Asset Configuration				
MIL1	b. Configuration baselines are used to configure assets at deployment	GENERIC.3	Verify, verify settings	
MIL2	c. The design of configuration baselines includes cybersecurity objectives	DER.2;	Secure design and implementation, require secure factory settings;	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
		DR.6, DGM.4, DGM.5	Secure operations, require application whitelisting	
3. Manage Changes to Assets				
MIL2	d. Change management practices address the full life cycle of assets (i.e., acquisition, deployment, operation, retirement)	DGM.8; DGM.3	Track, implement configuration management; Secure operations, maintain latest firmware	
MIL3	f. Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)	DGM.8	Track, implement configuration management	
4. Management Activities				
MIL2	a. Documented practices are followed for asset inventory, configuration, and change management activities	DGM.11, DGM.15, AMI.2, AMI.12, AMI.20, WAMPAC.8, DGM.5, DGM.9; AMI.21; AMI.24; DGM.7; WAMPAC12; AMI.21, AMI.27, DR.5, DR.6, DR.7	Track, implement configuration management; Track, track asset; Plan, define procedure; Profile, profile equipment; Secure design and implementation, design for trust; Secure design and implementation, configure for least functionality	
	d. Standards and/or guidelines have been identified to inform asset inventory, configuration, and change management activities	WAMPAC.4	Secure design and implementation, protect security configuration	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
MIL3	e. Asset inventory, configuration, and change management activities are guided by documented policies or other organizational directives	ET.3	Track, implement configuration management	
	h. Responsibility and authority for the performance of asset inventory, configuration, and change management activities are assigned to personnel	DER.1	Verify, require approval	
7.3 Identity and Access Management				
				• Inadequate anomaly tracking • Inadequate malware protection • Physical access to the device • Sensitive data protection vulnerability • Unnecessary system access • Use of insecure protocols • Weaknesses in authentication process or authentication keys
1. Establish and Maintain Identities				
MIL1	b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)	ET.9	Verify, verify EV owner	
MIL3	g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RM-1c)	AMI.3, AMI.6, AMI.9, AMI.10, AMI.22, AMI.23, AMI.30, AMI.31, DER.10, DER.11, DER.12, DER.17, DER.18, WAMPAC.10; AMI.13;	Authentication, require multi-factor authentication;	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
		DGM.10; WAMPAC.5, DR.4, DGM.11, DGM.15; AMI.23	Authentication, require second-level authentication; Authentication, require single sign-on; Verify, require 2-person rule; Verify, verify absence of hardcoded credentials	
2. Control Access				
MIL1	b. Access is granted to identities based on requirements	ET.9, ET.10, ET.11	Authentication, require PIN	
	c. Access is revoked when no longer required	AMI.21	Control access, require credential revocation	
MIL2	d. Access requirements incorporate least privilege and separation of duties principles	AMI.9, AMI.10, AMI.12, DER.10, DER.11, DER.12, ET.11, ET.13, DR.7; GENERIC.1	Control access, enforce least privilege; Isolate, require separation of duty	
3. Management Activities				
		AMI.3	Secure design and implementation, protect credentials	
MIL2	a. Documented practices are followed to establish and maintain identities and control access	GENERIC.1; AMI.3, AMI.13, AMI.15, DGM.3; ET.9, ET.10, ET.11; AMI.13	Plan, define procedure; Secure operations, Require video surveillance; Secure operations, require lockout; Verify, cross check	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
	b. Stakeholders for access and identity management activities are identified and involved	AMI.2, AMI.13	Secure operations, maintain anti-virus	
	d. Standards and/or guidelines have been identified to inform access and identity management activities	DGM.11, DGM.15	Secure operations, require strong passwords	
MIL3	e. Access and identity management activities are guided by documented policies or other organizational directives	DER.2, ET.6, ET.8, ET.9, ET.10, DGM.6, AMI.18; DER.14, DER.15, DER.19; AMI.8, AMI.11, DER.2, DER.7, DER.9, DER.14, DER.16, DER.18, DER.19, DER.20, DER.24, DR.3; AMI.3, AMI.12, DER.1, DER.2, DER.3, DER.10, DER.12, DER.16, DER.23, DER.25, WAMPAC.4, ET.1, ET.2, ET.15, DR.1, DR.5, DR.7, DGM.4, DGM.7, DGM.12, DGM.14; ET.11; AMI.2, AMI.9, AMI.10, AMI.12, AMI.25, AMI.29, WAMPAC.2, WAMPAC.6, WAMPAC.11, ET.11, DR.1, DR.2, DR.3, DR.4, DR.6, DGM.3, DGM.7; AMI.2, AMI.3, AMI.13, AMI.15, DR.1, DR.2, DR.3, DR.5, DGM.3, DGM.10, DGM.16;	Authenticate, authenticate devices; Authenticate, authenticate data sources; Authenticate, authenticate messages; Authenticate, authenticate users; Authenticate, require authentication; Control access, restrict network access; Control access, restrict physical access;	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
		AMI.1, AMI.2, AMI.3, DER.10, DER.12, DER.14, DER.15, DER.17, DER.18, DER.19, DER.20, DER.21, DER.24, DR.4, DR.6, Generic.1;	Control access, RBAC;	
		DER.2;	Control access, limit remote modification;	
		ET.6;	Control access, prevent modification;	
		WAMPAC.7;	Control access, require read-only access;	
		AMI.22, DER.10, DER.12, DER.25, WAMPAC.7, ET.16;	Control access, restrict application access;	
		WAMPAC.3, WAMPAC.4, WAMPAC.7, ET.11, ET.13, DR.1, DR.2, DR.4, DR.6, DR.7, DGM.4, DGM.11, DGM.15;	Control access, restrict remote access;	
		DER.23, WAMPAC.8;	Control access, restrict system access;	
		DGM.6;	Control access, restrict communication access;	
		AMI.3;	Control access, restrict configuration access;	
		WAMPAC.10, ET.4;	Control access, restrict database access;	
		AMI.18, DGM.3;	Control access, restrict device access;	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
		ET.11, ET.13, ET.15; AMI.3, AMI.9; WAMPAC.1, WAMPAC.3, WAMPAC.4; DGM.3; AMI.23, AMI.32; DER.10, WAMPAC.4	Control access, restrict file access; Control access, restrict internet access; Control access, restrict network services access; Control access, restrict port access; Secure operations, require password rule enforcement; Secure operations, change default credentials	
7.4 Threat and Vulnerability Management				
				• Inadequate anomaly tracking Inadequate patch management process
2. Reduce Cybersecurity Vulnerabilities				
MIL1	c. Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches)	ET.3, ET.16, DR.5, DR.7, DGM.4, DGM.5	Secure operations, maintain anti-virus	
MIL2	e. Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools)	AMI.12, AMI.17; DER.5;	Test, conduct penetration testing; Test, test after maintenance; Test, test before install;	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
		DER.5, WAMPAC.1, WAMPAC.6, WAMPAC.11, GENERIC.3, GENERIC.4, AMI.28; DER.3; ET.3, DGM.8, GENERIC.3	 Test, test for malware; Test, vulnerability scan before install	
	f. Identified cybersecurity vulnerabilities are analyzed and prioritized (e.g., NIST Common Vulnerability Scoring System could be used for patches; internal guidelines could be used to prioritize other types of vulnerabilities)	AMI.25	Track, implement configuration management	
MIL3	m. Cybersecurity vulnerability information is added to the risk register (RM-2j)	AMI.8; AMI.24, AMI.25, AMI.26; DER.5	Test, perform hardware acceptance testing; Test, perform security testing; Test, test after install	
	n. Risk monitoring activities validate the responses to cybersecurity vulnerabilities (e.g., deployment of patches or other activities)	DER.3	Verify, require on-going validation	
3. Management Activities				
MIL2	a. Documented practices are followed for threat and vulnerability management activities	DGM.3, DGM.4, DGM.5, AMI.25, DER.13, WAMPAC.2, ET.16, DR.5, DR.7	Secure operations, maintain patches	
7.5 Situational Awareness				
				• Business logic vulnerability • General logic error

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
				• Use of insecure protocols
1. Perform Logging				
MIL1	a. Logging is occurring for assets important to the function where possible	AMI.20	Audit, create audit log	
MIL2	b. Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])	AMI.1, AMI.2, AMI.3, AMI.10, AMI.31, DER.5, DER.6, DER.9, DER.17, DER.18, DER.21, DER.23, DER.24, ET.3, ET.9, ET.11, ET.13, ET.14, DGM.3, DGM.4, DGM.5, DGM.8	Audit, create audit log	
MIL3	e. Log data support other business and security processes (e.g., incident response, asset management)	DER.13	Audit, create audit log	
2. Perform Monitoring				
MIL1	b. Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event	Generic.1, ET.4; AMI.9, AMI.10, AMI.12, AMI.25, WAMPAC.4, WAMPAC.6, WAMPAC.11, DR.1, DR.2, DR.3, DGM.16; WAMPAC.5, WAMPAC.10; WAMPAC.3, WAMPAC.7; WAMPAC.2; WAMPAC.2	Detect, detect abnormal behavior; Detect, detect unauthorized access; Detect, detect unauthorized configuration; Detect, detect unauthorized connections; Detect, detect unauthorized devices; Detect, detect unusual patterns	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
MIL2	d. Alarms and alerts are configured to aid in the identification of cybersecurity events (IR-1b)	AMI.1, AMI.2, AMI.7, AMI.10, AMI.25, DER.6, DER.9, DER.11, DER.17, DER.18, DER.24, ET.2, ET.13, ET.15, DR.4, DGM.3, DGM.4, DGM.11, DGM.12, DGM.13, DGM.15, WAMPAC.7	Alert, generate alarms	
	e. Indicators of anomalous activity have been defined and are monitored across the operational environment	DGM.5, WAMPAC.7, AMI.7, AMI.31; AMI.1; ET.9; AMI.2, AMI.4, AMI.6, AMI.9, AMI.30, WAMPAC.2, ET.8, DR.3; AMI.2, ET.16, DR.1, DR.3, DR.4	Detect, detect abnormal behavior; Detect, detect anomalous commands; Detect, detect unauthorized use; Detect, detect unusual patterns; Detect, detect abnormal output	
MIL3	g. Monitoring requirements are based on the risk to the function	Generic.2	Alert, generate alerts	
	k. Alarms and alerts are configured according to indicators of anomalous activity	AMI.3; AMI.8	Alerts, generate alerts; Alerts, prioritize alarms	
7.7 Event and Incident Response, Continuity of Operations				
				• Business logic vulnerability • Inadequate continuity of operations or disaster recovery plan Inadequate incident response process
1. Detect Cybersecurity Events				
MIL2	d. Criteria are established for cybersecurity event detection	DGM.16	Secure operations, require tamper detection and response	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
	(e.g., what constitutes an event, where to look for events)			
3. Respond to Incidents and Escalated Cybersecurity Events				
MIL1	b. Responses to escalated cybersecurity events and incidents are implemented to limit impact to the function and restore normal operations	DGM.16	Secure operations, require tamper detection and response	
MIL2	d. Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident life cycle (e.g., triage, handling, communication, coordination, and closure)	DGM.9	Track, implement configuration management	
	f. Cybersecurity event and incident response plans address OT and IT assets important to the delivery of the function	GENERIC.2	Plan, define incident response plan	
MIL3	h. Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken	DGM.9	Analyze, review recovery response	
	m. Cybersecurity event and incident response plans are aligned with the function's risk criteria (RM-1c) and threat profile (TVM-1d)	AMI.15	Plan, emphasize security management	
	o. Restored assets are configured appropriately and inventory information is updated following execution of response plans	DGM.9	Plan, define policy	
4. Plan for Continuity				
MIL1	c. Continuity plans are developed to sustain and restore operation of the function	GENERIC.2	Plan, define contingency plan	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
MIL2	d. Business impact analyses inform the development of continuity plans	Generic.1	Plan, define procedure	
MIL3	i. The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly	AMI.15	Plan, define policy	
5. Management Activities				
MIL2	a. Documented practices are followed for cybersecurity event and incident response as well as continuity of operations activities	AMI.15	Plan, emphasize security management	
7.8 Supply Chain and External Dependencies Management				
2. Manage Dependency Risk				
		AMI.25	Plan, define procedure	
MIL1	a. Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed	DGM.8; DGM.8; DER.5	Ensure availability, require spares; Secure design and implementation, design for trust; Secure operations, require assured maintenance	
MIL2	i. Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements	Generic.4	Audit, perform audit	
7.9 Workforce Management				
				• Insufficient identity validation or background checks

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
				• Insufficiently trained personnel
2. Control the Workforce Life Cycle				
MIL1	a. Personnel vetting (e.g., background checks, drug tests) is performed at hire for positions that have access to the assets required for delivery of the function	DGM.8; WAMPAC.3, WAMPAC.5, WAMPAC.8; AMI.32, DER.3, DER.5, ET.3, DGM.2, DGM.8, DGM.10	Track, implement configuration management; Ensure availability, require redundancy; Verify, verify personnel	
MIL3	f. Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation	AMI.32, DER.3, DER.5, ET.3, DGM.2, DGM.8, DGM.10	Verify, verify personnel	
3. Develop Cybersecurity Workforce				
MIL1	a. Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities	AMI.2, AMI.13, DER.1, DER.2, DER.10, DER.11, DGM.15, Generic.2	Train, train personnel	
MIL2	c. Identified gaps are addressed through recruiting and/or training	AMI.9, DGM.10	Train, train personnel	
4. Increase Cybersecurity Awareness				
MIL1	a. Cybersecurity awareness activities occur	Generic.3	Train, train personnel	
7.10 Cybersecurity Program Management				
				• API abuse • Cryptographic vulnerability • Error handling vulnerability • Inadequate change and configuration management • Inadequate malware protection

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
				• Inadequate network segregation • Inadequate periodic security audits • Insufficient redundancy • Unneeded services running • Use of inadequate security architectures and designs • Use of insecure protocols • Weaknesses in authentication process or authentication keys
3. Establish and Maintain Cybersecurity Architecture				
MIL2	b. A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy	DER.10, DER.11, DER,12, Generic.2; WAMPAC.1, WAMPAC.4, WAMPAC.6, WAMPAC.11, DR.1, DR.2, DR.3, DGM.5, DER.14, DER.15, DER.17, DER.18, DER.21, GENERIC.2; WAMPAC.2; AMI.8, AMI.11, DER.4, WAMPAC.4, ET.7, ET.11, DGM.6, DGM.7, DGM.11, DGM.14, DGM.15, DGM.16; WAMPAC.2; AMI.9, AMI.10, DGM.4;	Control access, enforce restrictive firewall rules; Detect, require intrusion detection and prevention; Encrypt, encrypt application layer; Encrypt, encrypt communications path; Encrypt, encrypt link layer; Encrypt, require VPNs; Ensure availability, require fail-over;	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
		AMI.17; ET.12; DGM.1; DGM.1; DER.24, WAMPAC.1, ET.3, ET.9, ET.14; AMI.3, AMI.9, AMI.14, ET.3, DGM.11, DGM.15, GENERIC.2; AMI.4, AMI.14, AMI.22, AMI.29, DER.2, DR.2; AMI.4, AMI.5, AMI.16, WAMPAC.4; DER.2, DER.5, WAMPAC.2, DR.6, DR.7, DGM.3, GENERIC.3; DGM.14;	Ensure availability, require resiliency; Ensure availability, require synchronous functions; Ensure availability, require spread-spectrum radio; Isolate, isolate functions; Isolate, isolate networks; Secure design and implementation, require approved cryptographic algorithms; Secure design and implementation, require approved key management; Secure design and implementation, configure for least functionality; Secure design and implementation, design for trust; Secure operations, require secure boot loader; Verify, cross check;	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
		AMI.7, DER.13; AMI.7, DER.3; DR.1, DER.2; DR.7; DER.8, DER.9; WAMPAC.11; GENERIC.3; AMI.19; AMI.17	Verify, require acknowledgment; Verify, require message verification; Verify, require non-repudiation; Verify, verify correct operation; Verify, require periodic walk-downs; Verify, require reliable external time source; Verify, verify mode	
MIL3	d. Cybersecurity architecture is updated at an organization-defined frequency to keep it current	AMI.7	Secure operations, require secure remote firmware upgrade	
4. Perform Secure Software Development				
MIL2	a. Software to be deployed on assets that are important to the delivery of the function is developed using secure software development practices	AMI.26, AMI.27; DGM.7, DGM.12, WAMPAC.12;	Secure design and implementation, design for security; Secure design and implementation, design for trust; Test, conduct code review	

ES-C2M2		NESCOR Failure Scenarios	Common Mitigations	Common Vulnerabilities
		ET.3, DGM.8		

1.4 NISTIR 7628 Gap Analysis

The following table lists the NISTIR 7628 security requirements that were not associated with either the ES-C2M2 or the NIST CSF.

Table 1-4
NISTIR 7628 Gap Analysis

[The following information is extracted from the NISTIR 7628, the ES-C2M2, and the NIST CSF.]

NISTIR 7628 Security Requirements	Disposition in the Comparative Analysis Tables
Access Control (SG.AC)	
SG.AC-8: Unsuccessful Login Attempts	IAM-3a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AC-9: Smart Grid Information System Use Notification	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.AC-10: Previous Logon Notification	IAM-3a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AC-11: Concurrent Session Control	Not addressed
SG.AC-12: Session Lock	IAM-3a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AC-20: Publicly Accessible Content	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
Awareness and Training (SG.AT)	
SG.AT-4: Security Awareness and Training Records	WM-5a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AT-6: Security Responsibility Testing	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
Audit and Accountability (SG.AU)	
SG.AU-4: Audit Storage Capacity	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)

NISTIR 7628 Security Requirements	Disposition in the Comparative Analysis Tables
SG.AU-5: Response to Audit Processing Failures	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AU-8: Time Stamps	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.AU-9: Protection of Audit Information	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AU-10: Audit Record Retention	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AU-11: Conduct and Frequency of Audits	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AU-12: Auditor Qualification	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.AU-13: Audit Tools	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.AU-14: Security Policy Compliance	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.AU-16: Non-Repudiation	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
Security Assessment and Authorization (SG.CA)	
SG.CA-5: Security Authorization to Operate	Not addressed
Configuration Management (SG.CM)	
SG.CM-11: Configuration Management Plan	ACM-4a (NISTIR 7628 requirement not mapped to NIST CSF)
Continuity of Operations (SG.CP)	
SG.CP-7: Alternate Storage Sites	CPM-3b (NISTIR 7628 requirement not mapped to NIST CSF)

NISTIR 7628 Security Requirements	Disposition in the Comparative Analysis Tables
SG.CP-8: Alternate Telecommunication Services	CPM-3b (NISTIR 7628 requirement not mapped to NIST CSF)
SG.CP-11: Fail-Safe Response	IR-5a (NISTIR 7628 requirement not mapped to NIST CSF)
Identification and Authentication (SG.IA)	
Information and Document Management (SG.ID)	
SG.ID-2: Information and Document Retention	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.ID-3: Information Handling	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.ID-4: Information Exchange	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.ID-5: Automated Labeling	Not addressed
Incident Response (SG.IR)	
SG.IR-10: Smart Grid Information System Backup	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
Smart Grid Information System Development and Maintenance (SG.MA)	
SG.MA-2: Legacy Smart Grid Information System Updates	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
Media Protection (SG.MP)	
SG.MP-2: Media Sensitivity Level	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.MP-3: Media Marking	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
Physical and Environmental Security (SG.PE)	

NISTIR 7628 Security Requirements	Disposition in the Comparative Analysis Tables
SG.PE-5: Visitor Control	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.PE-6: Visitor Records	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.PE-7: Physical Access Log Retention	SA-4a (NISTIR 7628 requirement not mapped to NIST CSF)
SG.PE-8: Emergency Shutoff Protection	NISTIR 7628 requirement not mapped to ES-C2M2
SG.PE-9: Emergency Power	NISTIR 7628 requirement not mapped to ES-C2M2
SG.PE-11: Alternate Work Site	CPM-3b (NISTIR 7628 requirement not mapped to NIST CSF)
Planning (SG.PL)	
SG.PL-4: Privacy Impact Assessment	Not addressed
SG.PL-5: Security-Related Activity Planning	CPM-5d (NISTIR 7628 requirement not mapped to NIST CSF)
Security Program Management (SG.PM)	
SG.PM-2: Security Program Plan	RM-1c, CPM-5a, 5b, 5d, 5e (NISTIR 7628 requirement not mapped to NIST CSF)
SG.PM-3: Senior Management Authority	CPM-2b (NISTIR 7628 requirement not mapped to NIST CSF)
SG.PM-6: Security Authorization to Operate Process	Not addressed
Personnel Security (SG.PS)	
Risk Management and Assessment (SG.RA)	
Smart Grid Information System and Services Acquisition (SG.SA)	

NISTIR 7628 Security Requirements	Disposition in the Comparative Analysis Tables
SG.SA-2: Security Policy for Third Parties	IAM-2c, WM-3e, 3g (NISTIR 7628 requirement not mapped to NIST CSF)
SG.SA-4: Acquisitions	EDM-2f (NISTIR 7628 requirement not mapped to NIST CSF)
SG.SA-5: Smart Grid Information System Documentation	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SA-6: Software License Usage Restrictions	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SA-7: User-Installed Software	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
Smart Grid Information System and Communication Protection (SG.SC)	
SG.SC-2: Communications Partitioning	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SC-3: Security Function Isolation	CPM-3b (NISTIR 7628 requirement not mapped to NIST CSF)
SG.SC-4: Information Remnants	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SC-10: Trusted Path	Not addressed
SG.SC-11: Cryptographic Key Establishment and Management	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SC-12: Use of Validated Cryptography	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SC-13: Collaborative Computing	Not addressed
SG.SC-14: Transmission of Security Parameters	Not addressed
SG.SC-15: Public Key Infrastructure Certificates	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SC-17: Voice-Over Internet Protocol	Not addressed

NISTIR 7628 Security Requirements	Disposition in the Comparative Analysis Tables
SG.SC-20: Message Authenticity	CPM-3b (NISTIR 7628 requirement not mapped to NIST CSF)
SG.SC-21: Secure Name/Address Resolution Service	Not addressed
SG.SC-22: Fail in Known State	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SC-23: Thin Nodes	Not addressed
SG.SC-24: Honeypots	Not addressed
SG.SC-25: Operating System-Independent Applications	Not addressed
SG.SC-27: Heterogeneity	Not addressed
SG.SC-28: Virtualization Technique	Not addressed
SG.SC-29: Application Partitioning	Not addressed
SG.SC-30: Information System Partitioning	Not addressed
Smart Grid Information System and Information Integrity (SG.SI)	
SG.SI-6: Security Functionality Verification	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SI-8: Information Input Validation	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2
SG.SI-9: Error Handling	NISTIR 7628 requirement not mapped to NIST CSF or ES-C2M2

2
SUMMARY AND NEXT STEPS

The focus of this technical update is to provide guidance on the various cyber security regulations, guidelines, and security specifications that may be applicable to the electric sector. This document is not intended to provide new guidance but rather to provide information on how to navigate and relate the diverse existing guidance that is applicable to the electric sector. Utility management and external organizations, such as DOE and state PUCs, are requesting utilities to provide information on how they are meeting the various cyber security documents. The comparative analyses tables included in this technical update, and in the companion EPRI technical updates 3002004712, 3002003332, *Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)* and *3002003333, Risk Management in Practice - A Guide for the Electric Sector* provide guidance.

This is version 1.0 of this document, and version 1.0 of the companion documents. One of the objectives is to have a *baseline* set of tables that all utilities, research organizations, vendors, and others may use. Currently, utilities are developing their own tables or are requesting external companies to develop the tables. To move forward, it is important to have a set that is agreed to by everyone. The intent is to make this information publicly available and have utilities use the information and provide comments on the documents.

The next steps are to receive comments and recommendations and then revise the tables. This review and revision process will take several months, to ensure that all interested organizations have sufficient time to read and comment. Because it is not feasible to keep all the various tables synchronized when they are changed, the next phase will consider developing a database that contains all the information and making this publicly available.

3
REFERENCES

1. The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, Revision 1, September 2014 [report].

2. U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),* Version 1.1, February 2014 [government publication].

3. National Electric Sector Cybersecurity Organization Resource (NESCOR), *Electric Sector Failure Scenarios and Impact Analyses,* Version 2.0, June 2014 [report].

4. National Institute of Standards and Technology, NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, revision 4, April 2013 [government publication].

5. Nuclear Regulatory Commission, Regulatory Guidance 5.71, *Cyber Security Programs for Nuclear Facilities*, January 2010 [government publication].

6. Nuclear Energy Institute, NEI 08-09 Revision 6, *Cyber Security Plan for Nuclear Power Reactors*, April 2010 [government publication].

7. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014 [government publication].

4
ACRONYMS

CSF	Cybersecurity Framework
DOE	Department of Energy
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
MIL	Maturity Indicator Level
NARUC	National Association of Regulatory Utility Commissioners
NEI	Nuclear Energy Institute
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NRC	Nuclear Regulatory Commission
NRECA	National Rural Electric Cooperative Association
REV	Revision
SP	Special Publication

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

© 2014 Electric Power Research Institute (EPRI), Inc. All rights reserved.
Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

3002004712

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com