ELECTRIC POWER
RESEARCH INSTITUTE

Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

3002003332

Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

3002003332

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.

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.

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

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.

ACKNOWLEDGMENTS

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

Principal Investigator
A. Lee

The following organizations and individuals participated in the development of this report:

- Maurice Martin, Craig Miller, George Walker: National Rural Electric Cooperative Association (NRECA)
- Jason Christopher: Department of Energy
- John Fry, Fowad Muneer, Sean Storer: CF International
- James Stevens: Software Engineering Institute, Carnegie Mellon University

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

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

This report describes research sponsored by EPRI.

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:

Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). EPRI, Palo Alto, CA: 2014. 3002003332.

ABSTRACT

This technical update builds upon the previous evaluation framework, *Framework for Evaluating Cyber Security Posture for Power Delivery Systems*, EPRI Technical Update 3002001205, 2013 and provides guidance for performing a capability maturity assessment using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). Currently, the ES-C2M2 is intended to be applied at the organization level. Included in this document is application guidance that may be used by utilities to apply the ES-C2M2 to systems. This technical update addresses all ten domains in the ES-C2M2 and allocates NISTIR 7628 security requirements to objectives and maturity indicator levels (MILs) within each of the ten domains. The results of the system assessment may be used to determine the security posture of utility systems.

This document was developed jointly by several organizations, including EPRI, DOE, NRECA, Carnegie Mellon University, and several utilities, and is a companion to the *Risk Management in Practice - A Guide for the Electric Sector*, EPRI Technical Update 3002003333 also published in 2014.

Keywords
Cyber security
Cyber security maturity
Cyber security posture

EXECUTIVE SUMMARY

With the modernization of the electric grid, there is increased implementation of commercially available applications, operating systems, and communication protocols in control systems. With all this new digital technology, the potential for cyber security events has increased. In response to the changing threat environment and technologies, senior management and regulatory organizations are asking utility staff to provide information on the cyber security status of their control systems.

This technical update provides guidance for performing a capability maturity model assessment using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). Currently, the ES-C2M2 is intended for application at the organization level. This document includes application guidance that may be used by utilities to apply the ES-C2M2 to systems. The results of the system assessment may be used to determine the security posture of utility systems.

This document was developed jointly by several organizations, including the Electric Power Research Institute (EPRI), Department of Energy (DOE), The National Rural Electric Cooperative Association (NRECA), Carnegie Mellon University, and several utilities. It is a companion to *Risk Management in Practice - A Guide for the Electric Sector*, EPRI Technical Update 3002003333, published in December 2014.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
BACKGROUND

Cyber security is a priority for critical infrastructures, especially electric utilities. However, cybersecurity threats and concerns are constantly evolving and present complex, multifaceted challenges. Staying current with best practices requires constant attention to the changing technical landscape and a commitment to continuous improvement. There have been many efforts to support utilities in this endeavor and while they are each individually valuable, the number and diversity of guidance can create confusion since many address the same subject from different perspectives and use different nomenclature. This document is NOT an attempt to develop new guidance but rather to provide direction on how to apply existing guidance to information technology (IT) and operational technology (OT) systems.

The goal of this document is to focus on applying the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) methodology to *systems*. Initially, the ES-C2M2 was intended for organizations to determine their maturity levels in the ten domains. The next step is for organizations to apply the ES-C2M2 to IT and OT systems and determine the maturity levels in the domains. The results of the system assessments define the current security posture[1]. An organization may also develop *target* security postures for the different systems, identify gaps between the current and target postures, and determine the mitigation strategies that need to be implemented to address the gaps. The selection of mitigation strategies should be based on the overall risk management strategy, the level of acceptable residual risk, and the cyber security risk strategy.

As documented in the companion technical update, *Risk Management in Practice – A Guide for the Electric Sector*, the cyber security risk strategy is divided into three methodologies: maturity model, control-based, and compliance. This document focuses on the maturity model approach to system assessment as highlighted in Figure1-1 below. (Note: the descriptions of all the figure elements is included in the Risk Management document. Included here are the descriptions of the highlighted elements.)

The *maturity model methodology* (11) uses the *ES-C2M2* (8) document and the ES-C2M2 toolkit in the assessment. Currently, the ES-C2M2 is applied to *organizations* (16) rather than systems. To apply the ES-C2M2 to systems, *ES-C2M2 application guidance* (20) is used for *IT and OT systems* (17). The security requirements are defined in the *NISTIR 7628* (12) and the National Rural Electric Cooperative *(NRECA) Guidance* (19).

[1] The terms posture and profile are frequently used interchangeably. In this document, and the companion document, the term posture is used.

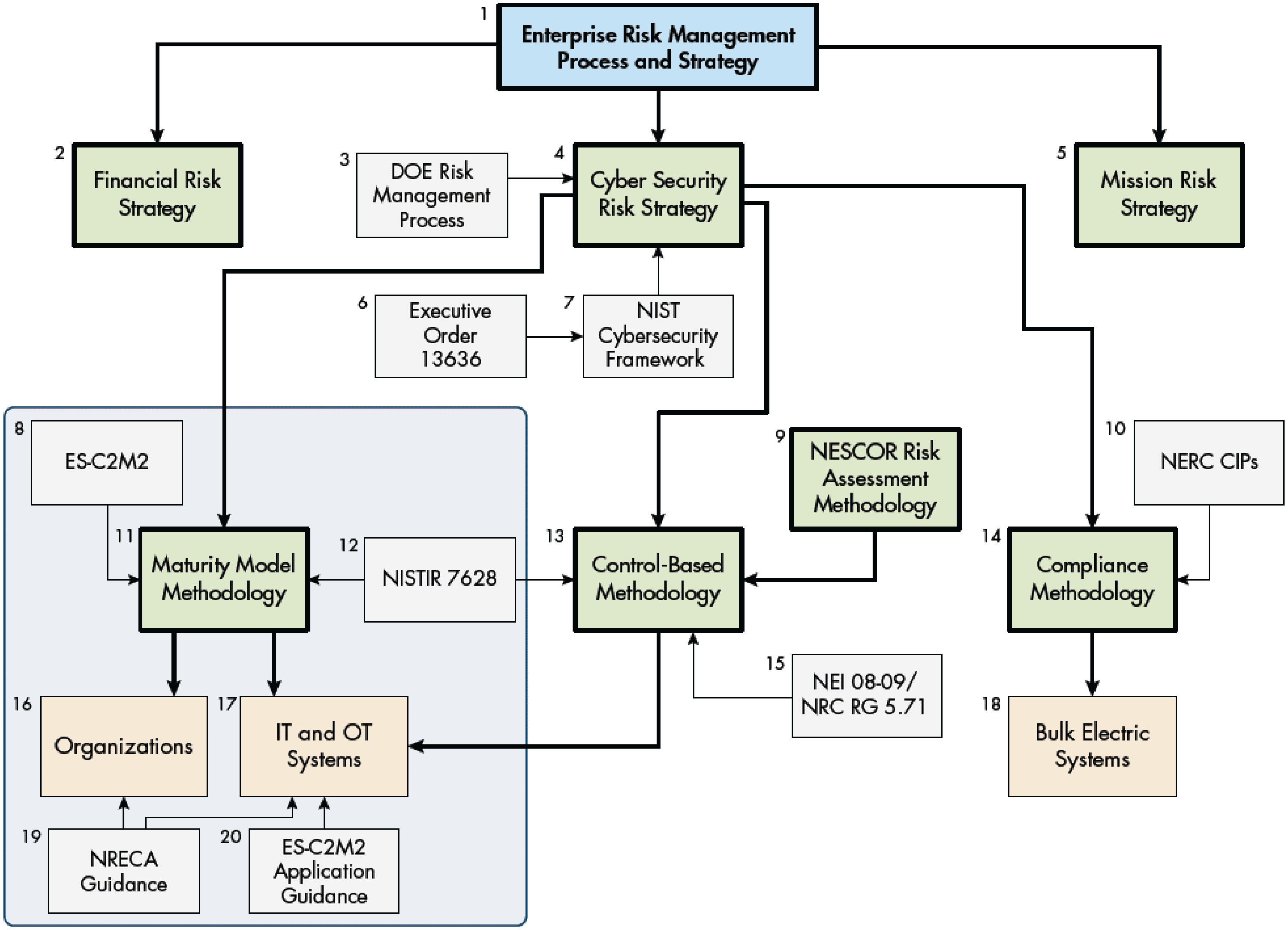

1
Enterprise Risk Management Process and Strategy
2
Financial Risk Strategy
3
DOE Risk Management Process
4
Cyber Security Risk Strategy
5
Mission Risk Strategy
6
Executive Order 13636
7
NIST Cybersecurity Framework
8
ES-C2M2
9
NESCOR Risk Assessment Methodology
10
NERC CIPs
11
Maturity Model Methodology
12
NISTIR 7628
13
Control-Based Methodology
14
Compliance Methodology
15
NEI 08-09/ NRC RG 5.71
16
Organizations
17
IT and OT Systems
18
Bulk Electric Systems
19
NRECA Guidance
20
ES-C2M2 Application Guidance

Figure 1-1
Enterprise Risk Management Process and Strategy – Maturity Model Methodology

1.1 Capability Maturity Model

A *capability maturity model* defines a set of characteristics and attributes that may be used to assess current capabilities and define capabilities for the future. This allows an organization to determine its current state, define a target state, and identify the capabilities that will be needed to meet the target state. The model may reference standards, policies, and best practices. To address cyber security in the electric sector, the Department of Energy (DOE), in collaboration with, for example, utilities, research organizations, federal agencies, and trade associations has developed the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). This model may be used by a utility of any size and configuration, for example, large vertically integrated utilities that include generation, transmission, and distribution, to small municipalities and cooperatives that purchase electricity from external sources and distribute it to their customers. The ES-C2M2 provides *descriptive* rather than *prescriptive* cyber security guidance and includes content from existing cyber security standards, guidelines, and recommendations. The ES-C2M2 content is at a high level of abstraction to allow each utility to apply the content based on the size and configuration of the organization. For cyber security systems, the current and target states may also be referenced as the current and target cyber security posture. As utilities develop their current and target cyber security postures and assess their systems they will need to identify the gaps in the existing systems that need to be mitigated. As utilities do not have unlimited resources, including both personnel and financial, prioritizing the identified gaps and the associated systems is critical.

The ES-C2M2 is organized into 10 *domains*. Each domain is further divided into *objectives* and each objective contains multiple *practices*. Included below is a summary of the ten domains extracted from the ES-C2M2. The information is included here for completeness.

1. **Risk Management**

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

2. **Asset, Change, and Configuration Management**

Manage the organization's IT and OT assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.

3. **Identity and Access Management**

Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

4. **Threat and Vulnerability Management**

Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

5. Situational Awareness

Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).

6. Information Sharing and Communications

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

7. Event and Incident Response, Continuity of Operations

Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

8. Supply Chain and External Dependencies Management

Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

9. Workforce Management

Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

10. Cybersecurity Program Management

Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

Finally, the practices are organized into three maturity indicator levels (MIL1 through MIL3). The MILs are hierarchical, that is, to achieve MIL2 within a domain, all the MIL1 practices must be met. In general, MIL1 practices may be implemented in an ad hoc manner; MIL2 practices represent an initial level of institutionalization; and MIL3 practices are further institutionalized and are now managed. (Note: this is a brief summary of the structure of the ES-C2M2. For a complete description, access the document at: http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf)

1.2 Content of This Technical Update

The ES-C2M2 is one tool that utilities may use to address the constantly changing cyber security technical environment and threat landscape. Other guidance, such as the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, the Department of Energy (DOE) *Electricity Subsector Cybersecurity Risk Management Process*, and the NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security* also address cyber security for electric sector. Each document has a different focus, perspective, and objective and all are revised over time. To assist the electric sector, this document and the companion EPRI document, *Risk Management in Practice - A Guide for the Electric Sector*, are intended to provide a framework to assist utilities in using the various cyber security documents in a coordinated manner. The goal is to provide a context for using the cyber security documents, rather than developing new guidance.

The focus of the EPRI Risk Management guidance is to define an overall enterprise risk management strategy, the three methodologies for implementing the guidance, and the applicable guidance/standards. The focus of this document is on the maturity model methodology and how to apply the ES-C2M2 at the system level, particularly in the operations environment, rather than at the organization level. The assessment results will be used in determining the security posture of the systems. To perform an ES-C2M2 system assessment, application guidance is needed. The application guidance is based on the security requirements in the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security* as applied to the ES-C2M2 objectives and security practices.

This technical update allocates the security requirements from the NISTIR 7628 to the ES-C2M2 practices and includes *application guidance* based on these security requirements. The application guidance is provided at the MIL level, rather than at the practice level, for each domain. In addition, this document provides guidance related to the Logical Interface Category (LIC) diagrams that are included in the NISTIR 7628, and the associated unique technical requirements (UTRs). Included with each LIC diagram is a summary of the ES-C2M2 practices that are associated with the listed UTRs.

Chapter 2 includes the application guidance for applying the ES-C2M2 to systems, chapter 3 includes the NISTIR 7628 logical interface diagrams and the application guidance, chapter 4 includes a gap analysis, and chapter 5 includes a summary and next steps. Included in Appendix A is a cross-reference between the NISTIR 7628 security requirements, the ES-C2M2 security practices, and the NISTIR 7628 assessment methods.

2
ES-C2M2 PRACTICES AND NISTIR 7628 SECURITY REQUIREMENTS

As discussed above, the ES-C2M2 currently is intended to be applied at the *organization* level. The following application guidance may be used to apply the ES-C2M2 to systems, particularly to control systems in the operations environment. The guidance is based on the security requirements from the NISTIR 7628 that are associated with the various security practices of the ES-C2M2. The guidance in this section is provided for each domain, objective, and MIL level. Included in Appendix A is Table A-1 that relates the NISTIR 7628 security requirements to each ES-C2M2 practice. Note: as described in the companion document, there is not a one-to-one relationship between the NISTIR 7628 security requirements and the ES-C2M2 practices. Therefore, some NISTIR 7628 security requirements may be listed multiple times.

2.1 NISTIR 7628 Security Requirements

The NISTIR 7628 is a catalog of security requirements. Therefore, a utility will need to select the applicable security requirements for each system and then tailor the requirements. The selection should be based on the priority of the system and the levels of the security objectives of confidentiality, integrity, and availability. The final list of security requirements should be based on these criteria and other criteria such as impact on performance, cost of the mitigation strategy, and availability of technical solutions. If there is a significant adverse impact on performance, a *compensating control* may be implemented. A compensating control is a cyber security control implemented as an alternative to a recommended control that provides equivalent or comparable control. When the security controls are implemented in the system, they will need to be assessed. The assessment methods are defined in the Smart Grid Interoperability Panel (SGIP) document *Guide for Assessing the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cyber Security*. The assessment methods are extracted from this document and listed below for completeness.

The assessment methods consist of examine, interview, and test, and define the nature of the assessor actions. An assessor may use any or all of the assessment methods listed below:

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

In all three assessment methods, the results are used to make specific determinations.

2.2 ES-C2M2 Assessment

An ES-C2M2 assessment may be performed using the toolkit that has been developed by DOE. The toolkit includes questions in the evaluation survey about practices in each domain. Responses are chosen from a four-point scale: Not Implemented, Partially Implemented, Largely Implemented, and Fully Implemented. The report that is developed presents the results in two views: the Objective view, which shows practice question responses by domain and objective; and the Domain view, which shows responses by Domains and MILs.

For ES-C2M2 system assessments, these same responses may be used in assessing the implementation of the tailored NISTIR 7628 security requirements. The results of the NISTIR 7628 assessments can be used as input to the ES-C2M2 system assessments. Using the same responses for the organization-level ES-C2M2 assessment and the system-level ES-C2M2 assessments should assist the utility in interpreting the results.

As described in the ES-C2M2, the current and target organization MILs for each domain and objective are based on the risk tolerance of the organization and the prioritization of the business units being assessed. A similar approach may be used for determining the current and target MILs for each domain and objective for a system.

Included below is *application guidance* based on Table A-1 that is included in Appendix A of this document. The guidance is provided at the maturity indicator level for each objective and domain and is tailored to the MIL. The information is a guideline and presented as a starting point for organizations as they begin to develop the ES-C2M2 program for assessing systems.

As specified in the NISTIR 7628, each security requirement is allocated to one of three categories: governance, risk, and compliance (GRC); common technical; or unique technical. The intent of the GRC requirements is to have them specified and addressed at the organization level. However, it may be necessary to augment and/or tailor these GRC requirements for specific systems or groups of systems. Many of the GRC requirements have technical components, and, where applicable, these are included in the descriptions below. The common technical requirements (CTRs) are applicable to all of the NISTIR 7628 LICs. The unique technical requirements (UTRs) are allocated to one or more of the NISTIR 7628 LICs. The UTRs and CTRs are typically allocated to a subset of the devices in a system, based on the security architecture.

The application guidance below focuses on the content of the NISTIR 7628 security requirements that is applicable to the MIL. As described previously, the ES-C2M2 and the NISTIR 7628 are intended for different purposes. Also, the ES-C2M2 MILs are hierarchical within each objective. In contrast, the NISTIR 7628 security requirements are organized within families and are not hierarchical. Consequently, a NISTIR 7628 security requirement may be allocated to a lower MIL and not to a higher MIL based on the specific content of the MIL. The NISTIR 7628 security requirement descriptions are organized by family category, for example, Access Control, Continuity of Operations, and Personnel Security.

2.3 Risk Management

1. Establish Cyber Security Risk Management Strategy

MIL1

No practice at MIL 1

MIL2

Security Program Management: The organization security program should include an overall risk management strategy and mission/business process definition. The risk management strategy should include the risk tolerance of the organization. The ES-C2M2 process should include an assessment of the implemented strategy in the control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

MIL3

Security Assessment and Authorization: The organization should: develop a security assessment plan, perform the assessment, produce a security assessment report, and provide this to management. The organization should establish a continuous monitoring strategy and implement a continuous monitoring program. The ES-C2M2 process should include an assessment of the implemented security requirements and the continuous monitoring process in the control systems. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Security Program Management: The organization should develop an organization-wide security program plan. The organization security program should include an overall risk management strategy and mission/business process definition. The risk management strategy should include the risk tolerance of the organization. The ES-C2M2 process should include an assessment of the implemented strategy in the control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

Risk Management and Assessment: The organization should develop a risk management plan; define the security impact level for the systems; and performs risk and vulnerability assessments. The ES-C2M2 process should include an assessment of the risk assessment methodology and the vulnerability analysis tools. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Information System and Services Acquisition: The developer should create and implements a security test and evaluation plan. The ES-C2M2 process should include an assessment of the risk approach implemented by the developer. The organization GRC requirement should be applied to the developer.

Information System and Information Integrity: The organization should develop and implement a flaw remediation process. For control systems, the implementation of automated patch management should be carefully considered in the ES-C2M2 assessment to ensure that there are no adverse impacts on operation. SG.SA-10 is a CTR that may be applied to a subset of the control system components.

2. Manage Cyber Security Risk

MIL1

Security Program Management: The organization security program should include an overall risk management strategy. The risk management strategy should include the risk tolerance of the organization. The ES-C2M2 process should include an assessment of the implemented strategy in the control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

MIL2

Security Program Management: The organization security program should include an overall risk management strategy. The risk management strategy should include the risk tolerance of the organization. The ES-C2M2 process should include an assessment of the implemented strategy in the control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems. (Note: the NISTIR 7628 requirement does not specifically include a network architecture that is referenced in the ES-C2M2.)

MIL3

Security Program Management: The organization security program should include risk management policies and procedures. The ES-C2M2 process should include an assessment of the policies and procedures as applied to the control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems. (Note: the NISTIR 7628 requirement does not specifically include a cyber-security architecture that is referenced in the ES-C2M2.)

3. Management Activities

MIL1

No practice at MIL 1

MIL2

Security Program Management: The organization security program should include an overall risk management strategy. The risk management strategy should include the risk tolerance of the organization. The ES-C2M2 process should include an assessment of the overall strategy for the control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

MIL3

Risk Management and Assessment: The organization should develop and implement a risk assessment security policy. The ES-C2M2 process should include an assessment of the referenced standards, guidelines, and regulations. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Physical and Environment Security: The organization should develop and implement a physical and environmental security policy. The ES-C2M2 process should include an assessment of the referenced standards, guidelines, and regulations. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Security Program Management: The organization security program should include an overall risk management strategy. The risk management strategy should include assignment of responsibilities, a list of the applicable policies and directives, and be reviewed at regular intervals. The ES-C2M2 process should include an assessment of the overall strategy for the control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

2.4 Asset, Change and Configuration Management

1. Manage Asset Inventory

MIL1

Configuration Management: The organization should develop and maintain baseline configurations and component inventories for the control systems. The ES-C2M2 process should include an assessment of the baselines and component inventories for completeness and accuracy. The GRC requirements should be applied at the system level, and not at the organization level.

Continuity of Operations: The organization should identify and operate an alternate control center to ensure the resumption of system operations for critical functions. The ES-C2M2 process should include an assessment of the center configuration and any applicable contracts. The GRC requirement should address priority control systems.

Risk Management and Assessment: The organization should consider the security impact level when identifying assets that are important for specific functions. The ES-C2M2 process should include a review of the security impact level criteria and application to the control systems. The GRC requirement should be defined at the organization level.

Smart Grid Information System and Communication Protection: The organization should apply the resource priority criteria in identifying assets that are important for specific functions. The ES-C2M2 process should include a review of the resource priority criteria assigned to the control systems and components. SG.SC-6 is a UTR that may be applied to a subset of the control system components.

MIL2

Configuration Management: The organization should develop and maintain component inventories for the control systems. The ES-C2M2 process should include an assessment of the component inventories to ensure that the ES-C2M2 specified attributes, e.g., location, asset owner, security requirements, are included. The GRC requirement should be applied at the system level, and not at the organization level.

Risk Management and Assessment: The organization should consider the security impact level when identifying assets that are important for specific functions. The ES- C2M2 process should include an assessment of the attributes of the assets to ensure that the ES-C2M2 specified attributes, e.g., location, asset owner, security requirements, are included. The GRC requirement should be defined at the organization level.

Information System and Communication Protection: The organization should apply the resource priority criteria in identifying assets that are important for specific functions. The ES-C2M2 process should include an assessment of the attributes of the assets to ensure that the ES-C2M2 specified attributes, e.g., location, asset owner, security requirements, are included. SG.SC-6 is a UTR that may be applied to a subset of the control system components.

Continuity of Operations: The organization should identify the prioritized assets that may need to be implemented in the alternate control center. The ES-C2M2 process should include an assessment of the prioritized assets to ensure that critical functions are addressed. The GRC requirement should address prioritized control systems.

MIL3

Security Assessment and Authorization: The organization should identify and document control system connections to other systems within and external to the organization. The ES-C2M2 process should review the documentation for completeness and accuracy. The GRC requirement should address the control systems.

Configuration Management: The organization should develop, maintain, and keep current component inventories of the connected IT and OT assets. The ES-C2M2 process should include a review of the component inventories to ensure that they are current and at the appropriate level of granularity. The GRC requirement should be developed and applied at the system level, and not at the organization level.

Security Program Management: The organization should develop an overall security architecture. The ES-C2M2 process should ensure that the security architecture includes and addresses control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

Smart Grid Information System and Services Acquisition: The organization should consider supply chain issues for assets that are critical to the delivery of the function. The ES-C2M2 process should include a review of the supply chain mitigation strategies. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

2. Manage Asset Configuration

MIL1

Configuration Management: The organization should develop and maintain baseline configurations and configuration settings for the groups of control systems. The ES-C2M2 process should include an assessment of the baseline inventories and configuration settings to ensure consistency in configurations and in deployed assets. The GRC requirements should be developed and applied at the system level, and not at the organization level.

Smart Grid Information System and Services Acquisition: The developer should create and implement a configuration management process. The ES-C2M2 process should include an assessment of the configuration management process to ensure that the assets are consistently configured. The organization GRC requirement should be applied to the developer.

MIL2

Configuration Management: The organization should configure the control systems for least functionality. The ES-C2M2 process should include an assessment of the systems to ensure that only essential services are implemented and that unnecessary functions, ports, services, and protocols are restricted. The ES-C2M2 process should also include a review of the configuration baseline designs to ensure cyber security objectives are included. SG.CM-7 is a CTR that may be applied to a subset of the control system components.

MIL3

Configuration Management: The organization should develop and maintain baseline configurations for the groups of control systems. The ES-C2M2 process should include an assessment to ensure the baselines are reviewed and updated and that the configurations are monitored. The GRC requirements should be developed and applied at the system level, and not at the organization level.

3. Manage Changes to Assets

MIL1

Configuration Management: The organization should develop and maintain a configuration change control process and monitor the configuration changes. The ES-C2M2 process should include an assessment to ensure that configuration changes are evaluated before implementation. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

The organization should log configuration settings, update the component inventory, and track the addition of control system equipment. The ES-C2M2 process should include a review of the logs and documentation to determine if the procedures are being followed. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System Development and Maintenance: The organization should perform and review maintenance for control systems, including assessing the impact of changes. The ES-C2M2 process should include a review of the maintenance process and records and ensure that changes are logged.

The organization should log configuration settings, update the component inventory, and track the addition of control system equipment. The ES-C2M2 process should include a review of the logs and documentation to determine if the procedures are being followed.

The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Physical and Environmental Security: The organization should develop delivery and removal procedures for control systems. The ES-C2M2 process should include a review of these procedures. The organization should log configuration settings, update the component inventory, and track the addition of control system equipment. The ES-C2M2 process should include a review of the logs and documentation to determine if the procedures are being followed. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Services Acquisition: The developer configuration management process should include logging changes. The ES-C2M2 process should include an assessment of the configuration management process to ensure that the changes are logged. The organization GRC requirement should be applied to the developer.

MIL2

Configuration Management: The organization should develop and maintain baseline configurations and configuration change control; manage the addition, removal, and disposal of equipment; and manage factory default settings for the groups of control systems. The ES-C2M2 process should include an assessment to ensure that the procedures are followed and that the baselines and settings are correctly managed. The GRC requirements should be specified for the control systems.

Media Protection: The organization should sanitize control system media before disposal or release. The ES-C2M2 process should ensure that the medial sanitization and disposal actions are performed throughout the asset life cycle. The GRC requirement should be defined at the organization level.

Physical and Environmental Security: The organization should control system components entering and exiting the facility. The ES-C2M2 process should ensure that records are maintained. The GRC requirements should be specified for the control systems.

Information System and Services Acquisition: The organization should define and implement security engineering practices and system development lifecycle methodologies. The ES-C2M2 process should include an assessment of these practices and methodologies. The GRC requirement should be defined at the organization level.

The developer should create and implements a security test and evaluation plan and create and implement a configuration management process. The ES-C2M2 process should include an assessment to ensure that the developer plan and process address all phases of the system life cycle. The organization GRC requirement should be applied to the developer.

MIL3

Configuration Management: The organization should develop and maintain baseline configurations for the control systems and maintain a configuration change control process and monitor the configuration changes. The ES-C2M2 process should include an assessment to ensure that the changes are tested prior to deployment. The GRC requirements should be developed and applied at the system level, and not at the organization level.

Smart Grid Information System Development and Maintenance: The organization should document maintenance for control systems. The ES-C2M2 process should include a review of the maintenance records and ensure that the change logs include cyber security impact. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

4. Management Activities

MIL1

No practice at MIL 1

MIL2

Configuration Management: The organization should have documented practices for the following configuration management activities: configuration change control; monitoring configuration change; access restrictions for configuration change; configuration settings; component inventory; addition, removal, and disposal of equipment; factory default settings management; and configuration management plan. The roles responsible for component inventory should be documented. The ES-C2M2 process should include an assessment that the practices are documented and followed. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Media Protection: The organization should sanitize control system media before disposal or release. The ES-C2M2 process should ensure that the medial sanitization and disposal procedures and guidelines/standards are developed and used. The GRC requirement should be defined at the organization level.

Physical and Environmental Security: The organization should develop delivery and removal procedures for control systems. The ES-C2M2 process should include a review of these procedures. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Services Acquisition: The developer should create and implement a configuration management process. The ES-C2M2 process should include an assessment of the configuration management process to ensure that the assets are consistently configured. The organization GRC requirement should be applied to the developer.

Smart Grid Information System Development and Maintenance: The organization should have maintenance tools, authorized maintenance personnel, and spare parts for timely maintenance. The ES-C2M2 process should include a review of the maintenance process and ensure that adequate resources are provided. The GRC requirements should be specified for the control systems.

MIL3

Configuration Management: The organization should have documented practices for the following configuration management activities: configuration change control; monitoring configuration change; configuration settings; component inventory; addition, removal, and disposal of equipment; factory default settings management; and configuration management plan. The ES-C2M2 process should include an assessment that organization directives or documented polices guide the configuration management practices. The GRC requirements should be specified for the control systems.

Physical and Environmental Security: The organization physical and environmental security policy, emergency shutoff protection, emergency power, and location of information assets should be based on standards and/or guidelines. The ES-C2M2 process should include an assessment of the policy and implementations to ensure that applicable standards and/or guidelines are applied. The GRC requirements should be specified for the control systems.

2.5 Identity and Access Management

1. Establish and Maintain Identities

MIL1

Access Control: The organization should develop and implement account management, including deprovisioning. The ES-C2M2 assessment should include a review to ensure that accounts and privileges are defined and assigned to individuals and devices based on need and removed when no longer needed. The GRC requirement should be developed and applied at the system level, and not at the organization level.

The organization should develop policies and procedures for passwords. The ES-C2M2 assessment should review and test the password procedures. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

The organization should restrict access to control systems. The ES-C2M2 assessment should include a test of access to the control systems and/or a review of the test results. SG.AC-19 is a CTR that may be applied to a subset of the control system components.

Identification and Authentication: The organization should define and assign identification and authentication credentials to users and devices. The ES-C2M2 assessment should include a test and review of these assignments. SG.IA-4 and SG.IA-5 are UTRs that may be applied to a subset of the control system components.

The organization should receive authorization from a management authority to assign identifiers. The ES-C2M2 process should include a review of this authorization. The GRC requirements should be developed and applied at the system level, and not at the organization level.

MIL2

Access Control: The organization should implement account management that includes reviewing the accounts on an organization-defined frequency and when users are terminated, transferred, or the usage changes. The ES-C2M2 assessment should include a review of the account management procedures to ensure that the requirements are met. The GRC requirements should be developed and applied at the system level, and not at the organization level.

Identification and Authentication: The organization should implement authenticator management to ensure that credentials are associated with the correct individual/device. The ES-C2M2 assessment should include a review of the procedures and the identification and authentication tests. The GRC requirements should be developed and applied at the system level, and not at the organization level. SG.IA-4 and SG.IA-5 are UTRs that may be applied to a subset of the control system components.

MIL3

Identification and Authentication: The organization should implement user identification and authentication that includes multifactor authentication. The ES-C2M2 assessment should include a review to ensure that multifactor authentication is included. SG.IA-4 is a UTR that may be applied to a subset of the control system components.

2. Control Access

MIL1

Access Control: The organization should develop and implement access enforcement, access control for remote access, remote session termination, remote access, permitted actions without identification or authentication, and remote access for portable and media devices. The ES-C2M2 assessment should include a review of the applicable documentation and testing of the remote session termination and remote access controls. The GRC requirements should be developed and applied at the system level, and not at the organization level. SG.AC-13, SG.AC-14, and SG.AC-15 are UTRs that may be applied to only a subset of the control system components.

Smart Grid Information System Development and Maintenance: The organization should develop and implemented policies and procedures for remote maintenance based on requirements. The ES-C2M2 assessment should include a review of the remote maintenance policies and procedures and ensure that access is granted based on requirements and that revoking access is included. The GRC requirement should be developed and applied at the system level, and not at the organization level.

Media Protection: The organization should develop procedures and processes for media storage and transport. The ES-C2M2 assessment should review the procedures to ensure that only authorized individuals perform the activities. The GRC requirement should be defined at the organization level.

Physical and Environmental Security: The organization should develop and implement physical access control procedures and authorizations. The ES-C2M2 assessment should include a review of the procedures and a test of the physical access controls. The GRC requirements should be specified for the control systems.

MIL2

Access Control: The organization should develop and implement separation of duties and least privilege mitigations on the control systems. The ES-C2M2 assessment should include a review of the documentation and a test of the controls. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

The organization should review remote access requests. The ES-C2M2 assessment should include a review of the documentation to ensure that the asset owner approves the remote access. The GRC requirements should be specified for the control systems.

Smart Grid Information System Development and Maintenance: The organization should develop and implemented policies and procedures for remote maintenance based on requirements. The ES-C2M2 assessment should include a review of the remote maintenance policies and procedures and ensure that access is granted by the asset owner. The GRC requirement should be developed and applied at the system level, and not at the organization level.

Physical and Environmental Security: The organization should develop and implement physical access control procedures and authorizations. The ES-C2M2 assessment should include a review of the accounts such as root, administrative, guest, etc. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

Physical and Environmental Security: The organization should develop and implement physical access control procedures and authorizations. The ES-C2M2 assessment should ensure the procedures include an organizationally defined review frequency. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System Development and Maintenance: The organization should develop and implemented policies and procedures for remote maintenance based on risk. The ES-C2M2 assessment should include a review of the remote maintenance policies and procedures and ensure that access is granted based on risk. The GRC requirement should be developed and applied at the system level, and not at the organization level.

3. Management Activities

MIL1

No practice at MIL 1

MIL2

Access Control: The organization should implement unsuccessful login attempts, previous logon notification, and session lock controls. The ES-C2M2 process should include tests of the controls. SG.AC-8 is a CTR and SG.AC-10 and SG.AC-12 are UTRs that may be applied to only a subset of the control system components.

MIL3

Access Control: The organization should develop access control procedures that are based on policy. The ES-C2M2 process should review the access control procedures and ensure they address policy. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Identification and Authentication: The organization should develop identification and authentication procedures that are based on policy. The ES-C2M2 process should review the identification and authentication procedures and ensure they address policy. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

2.6 Threat and Vulnerability Management

1. Identify and Respond to Threats

MIL1

Awareness and Training: The organization should establish and maintain contact with security groups to gather threat information. The ES-C2M2 process should include a review of the information sources. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Information Integrity: The organization should gather threat information from external sources. The ES-C2M2 process should include a review of the information sources. The GRC requirements should be specified for the control systems.

Risk Management and Assessment: The organization should conduct risk assessments taking into account threat sources. The ES-C2M2 assessment should include a review of the risk assessment process and how this addresses threat information. The GRC requirements should be specified for the control systems.

Access Control: The organization should implement separation of duties and least privilege to address threats. The ES-C2M2 assessment should include a review of the documentation and testing of the controls. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Communication Protection: The organization should implement, if applicable, denial-of-service protection, boundary protection, communication integrity, communication confidentiality, cryptography, and confidentiality of information at rest to address prioritized threats. The ES-C2M2 assessment should include testing of these controls. SG.SC-12 is a CTR and SG.SC-5, SG.SC-7, SG.SC-8, SG.SC-9, and SG.SC-26 are UTRs. These requirements may be applied to a subset of the control system components.

MIL2

Risk Management and Assessment: The organization should define the security impact level for the control systems and perform risk assessments. The ES-C2M2 process should include an assessment to ensure that threat profiles have been developed. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Information Integrity: The organization should gather threat information from external sources. The ES-C2M2 process should include a review of the information sources to ensure they are monitored and prioritized. The GRC requirements should be specified for the control systems.

Security Program Management: The organization security program should include an overall risk management strategy that includes analyzing and prioritizing threats. The ES-C2M2 process should include an assessment of the implemented strategy in the control systems. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

MIL3

There are no applicable NISTIR 7628 security requirements.

2. Reduce Cybersecurity Vulnerabilities

MIL1

Awareness and Training: The organization should establish and maintain contact with security groups to gather vulnerability information. The ES-C2M2 process should include a review of the information sources. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Information Integrity: The organization should gather vulnerability information from external sources. The ES-C2M2 process should include a review of the information sources to ensure they are monitored and prioritized. The GRC requirements should be specified for the control systems.

The organization should develop and implement a flaw remediation process. For control systems, the flaw remediation should be carefully considered in the ES-C2M2 assessment to ensure that there are no adverse impacts on operations. SG.SI-2 is a CTR and may be applied to a subset of the control system components.

Security Assessment and Authorization: The organization should develop and implement security assessments and continuous monitoring activities. The ES-C2M2 process should include a review of the procedures and ensure that vulnerabilities are considered. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Risk Management and Assessment: The organization should develop and implement a vulnerability assessment process. The ES-C2M2 process should include a review of the vulnerability process to assess its effectiveness. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Services Acquisition: The developer should develop and implement a security test and evaluation plan. The ES-C2M2 process should include a review of the developers plan to ensure that vulnerabilities are assessed. SG.SA-10 is a CTR and should be applied to the developer.

Access Control: The organization should implement separation of duties and least privilege to address vulnerabilities. The ES-C2M2 assessment should include a review of the documentation and testing of the controls. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Communication Protection: The organization should implement, if applicable, denial-of-service protection, boundary protection, communication integrity, communication confidentiality, cryptography, and confidentiality of information at rest to address prioritized vulnerabilities. The ES-C2M2 assessment should include testing of these controls. SG.SC-12 is a CTR and SG.SC-5, SG.SC-7, SG.SC-8, SG.SC-9, and SG.SC-26 are UTRs. These requirements may be applied to a subset of the control system components.

MIL2

Awareness and Training: The organization should establish and maintain contact with security groups to gather vulnerability information. The ES-C2M2 process should include a review of the information sources to ensure they are monitored. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Security Assessment and Authorization: The organization should develop and implement security assessments and continuous monitoring activities. The ES-C2M2 process should ensure that vulnerability assessments are performed. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Risk Management and Assessment: The organization should perform vulnerability assessments. The ES-C2M2 process should include a review of the vulnerability process to assess its effectiveness and the prioritization of vulnerabilities. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Services Acquisition: The developer should execute vulnerability assessments. The ES-C2M2 process should include a review of the developer's vulnerability assessment tests and results. SG.SA-10 is a CTR and should be applied to the developer.

Smart Grid Information System and Information Integrity: The organization should monitor external sources for vulnerability information. The ES-C2M2 process should include a review of the information sources to ensure they are monitored. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

Security Assessment and Authorization: The organization should develop and implement security assessments and continuous monitoring activities. The ES-C2M2 process should include a review of the procedures to ensure that prioritized control systems are assessed and that risk is considered. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Risk Management and Assessment: The organization should develop and implement a vulnerability assessment process and monitor the mitigation strategies. The ES-C2M2 process should include a review of the vulnerability process to assess its effectiveness. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Services Acquisition: The developer should develop and implement a security test and evaluation plan. The ES-C2M2 process should include a review of the developers plan to ensure that vulnerabilities are assessed. SG.SA-10 is a CTR and should be applied to the developer.

Smart Grid Information System and Information Integrity: The organization should develop and implement a flaw remediation process. For control systems, flaw remediation should be carefully considered in the ES-C2M2 assessment to ensure that there are no adverse impacts on operations. SG.SI-2 is a CTR and may be applied to a subset of the control system components.

(Note: to meet one practice in the ES-C2M2, the vulnerability assessments need to be performed by individuals that are independent of the operations.)

3. Management Activities

MIL1

No practice at MIL 1

MIL2

Risk Management and Assessment: The organization should conduct a risk assessment, update the risk assessment plan, and perform vulnerability assessment to manage vulnerabilities. The ES-C2M2 process should include an assessment of the various processes. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Information Integrity: The organization should develop and implement a flaw remediation process to address threats and vulnerabilities. For control systems, the flaw remediation should be carefully considered in the ES-C2M2 assessment to ensure that there are no adverse impacts on operations. SG.SI-2 is a CTR and may be applied to a subset of the control system components.

MIL3

Risk Management and Assessment: The organization should develop and implement a risk assessment policy that addresses threats and vulnerabilities. The ES-C2M2 process should include a review of this policy. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

2.7 Situational Awareness

1. Perform Logging

MIL1

Audit and Accountability: The organization should identify events to be audited for assets that are important for the function. The ES-C2M2 process should assess the auditable events to ensure they address risk. The GRC requirements should be specified for the control systems.

MIL2

Audit and Accountability: The organization should identify events to be audited for assets that are important for the function, generate audit records, and review and analyze the audit records. The ES-C2M2 process should include a review of the audit generation criteria and the audit records. The GRC requirements should be specified for the control systems.

MIL3

Audit and Accountability: The organization should generate audit records, and review and analyze the audit records. The ES-C2M2 process should include a review of the audit generation criteria and the audit records to ensure they are based on risk. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

2. Perform Monitoring

MIL1

Access Control: The organization should define, implement and monitor remote access, wireless access, and portable and mobile device access. The ES-C2M2 process should include a review of the logging records for anomalous behavior. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems. SG.AC-15 is a UTR and may be applied to a subset of the control system components.

Audit and Accountability: The organization should review and analyze audit records at a defined frequency. The ES-C2M2 process should include a review of the audit review procedures for the review periods. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Security Assessment and Authorization: The organization should establish a continuous monitoring process. The ES-C2M2 process should include a review of the monitoring process for the review periods. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Configuration Management: The organization should establish a process to monitor configuration changes. The ES-C2M2 assessment should review this process to ensure that operational environments are monitored for anomalous activity. The GRC requirements should be specified for the control systems.

Physical and Environmental Security: The organization should establish a process to monitor physical access. The ES-C2M2 assessment should review this process to ensure that physical access is monitored for anomalous activity. The GRC requirements should be specified for the control systems.

Personnel Security: The organization should establish a personnel security process for employees, contractors, and third party to monitor activities. The ES-C2M2 assessment should review this process to ensure that personnel activity is monitored. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Communication Protection: The organization should implement system monitoring at the external boundary of the system and monitoring of the use of mobile code. The ES-C2M2 process should include a review of the monitoring records to identify anomalous behavior. SG.SC-7 is a UTR and SG.SC-16 is a CTR. These requirements may be applied to a subset of the control system components.

Smart Grid Information System and Information Integrity: The organization should implement malicious code and spam protection and monitor system events to detect anomalous events. The ES-C2M2 process should include a review of the malicious code protection mechanisms and the monitoring events. For control systems, the implementation of malicious code and spam protection should be carefully considered in the ES-C2M2 assessment to ensure that there are no adverse impacts on operation. The GRC requirements should be specified for the control systems.

MIL2

Audit and Accountability: The organization should generate audit records, and review and analyze the audit records. The ES-C2M2 process should include a review for timely review of the data. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Access Control: The organization should define, implement and monitor remote access, wireless access, and portable and mobile device access. The ES-C2M2 process should include a review for indicators of anomalous activity. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems. SG.AC-15 is a UTR and may be applied to a subset of the system components.

Configuration Management: The organization should establish a process to monitor configuration changes. The ES-C2M2 assessment should review this process to ensure that indicators of anomalous activity are defined and monitored. The GRC requirements should be specified for the control systems.

Physical and Environmental Security: The organization should establish a process to monitor physical access. The ES-C2M2 assessment should review this process to ensure that indicators of anomalous activity are defined and monitored. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Personnel Security: The organization should establish a personnel security process for employees, contractors, and third party to monitor activities. The ES-C2M2 assessment should review this process to ensure that indicators of anomalous activity are defined and monitored. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Communication Protection: The organization should implement system monitoring at the external boundary of the system and monitoring of the use of mobile code. The ES-C2M2 process should include a review of the configuration to ensure that indicators of anomalous behavior are implemented and monitored. SC-7 is a UTR and SG.SC-16 is a CTR and may be applied to a subset of the system components.

Smart Grid Information System and Information Integrity: The organization should implement malicious code and spam protection and monitor system events to detect anomalous events. For control systems, the implementation of malicious code and spam protection should be carefully considered in the ES-C2M2 assessment to ensure that there are no adverse impacts on operation. The ES-C2M2 process should include a review of the malicious code protection mechanisms and the monitoring events. SG.SI-3 and SG.SI-4 are CTR and may be applied to a subset of the system components.

The organization should implement integrity controls. The ES-C2M2 process should include a review of the integrity controls to ensure they are applied to sensitive information. SG.SI-7 is a UTR and may be applied to a subset of the system components.

MIL3

Access Control: The organization should define, implement and monitor remote access, wireless access, and portable and mobile device access. The ES-C2M2 process should include a review to ensure that the controls are based on risk and identify anomalous behavior. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems. SG.AC-15 is a UTR and may be applied to a subset of the system components.

Security Assessment and Authorization: The organization should establish a continuous monitoring process. The ES-C2M2 process should include a review of the monitoring process to ensure that risk is considered. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Communication Protection: The organization should implement system monitoring at the external boundary of the system and monitoring of the use of mobile code. The ES-C2M2 process should include a review of the configuration to ensure that indicators of anomalous behavior are implemented and monitored. SG.SC-7 is a UTR and SG.SC-16 is a CTR. These requirements may be applied to a subset of the system components.

Configuration Management: The organization should establish a process to monitor configuration changes. The ES-C2M2 assessment should review this process to ensure that indicators of anomalous activity are monitored. The GRC requirements should be specified for the control systems.

Physical and Environmental Security: The organization should establish a process to monitor physical access. The ES-C2M2 assessment should review this process to ensure that indicators of anomalous activity are defined and monitored. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Information Integrity: The organization should implement malicious code and spam protection and monitor system events to detect anomalous events. For control systems, the implementation of malicious code and spam protection should be carefully considered in the ES-C2M2 assessment to ensure that there are no adverse impacts on operation. The ES-C2M2 process should include a review of the malicious code protection mechanisms to ensure continuous monitoring is performed. SG.SI-3 and SG.SI-4 are CTR and may be applied to a subset of the system components.

The organization should implement integrity controls. The ES-C2M2 process should include a review of the integrity controls to ensure they are applied to sensitive information. SG.SI-7 is a UTR and may be applied to a subset of the system components.

3. Establish and Maintain a Common Operating Picture (COP)

MIL1

No practice at MIL 1

MIL2

There are no applicable NISTIR 7628 security requirements.

MIL3

Audit and Accountability: The organization should implement audit report generation. The ES-C2M2 process should include a review of reports to ensure they provide information on the state of cyber security. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

4. Management Activities

MIL1

No practice at MIL 1

MIL2

Audit and Accountability: The organization should define audit record content, address audit storage capacity, implement mechanisms for audit processing failures and protection of audit information, specify frequency of audits, and select audit tools. The ES-C2M2 process should include a review of the procedures and mechanisms. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems. SG.AU-3, SG.AU-4, and SG.AU-9 are CTRs and may be applied to a subset of the system components.

Physical and Environmental Security: The organization should implement physical access controls for visitors, maintain visitor records, and define time frames for retaining the physical access logs. The ES-C2M2 process should include a review of the visitor records to ensure they contain the required information. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

Audit and Accountability: The organization should implement auditing policies and procedures. The ES-C2M2 process should include a review to ensure that applicable organization directives, standards, and guidelines are used in developing and reviewing the audit policies and procedures. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Information Integrity: The organization should develop information system and information integrity policy and procedures. The ES-C2M2 process should ensure that applicable standards and guidelines are considered. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

2.8 Information Sharing and Communications

1. Share Cybersecurity Information

MIL1

Awareness and Training: The organization should establish and maintain contact with security groups to gather threat information. The ES-C2M2 process should include a review of the information sources. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Audit and Accountability: The organization should identify the management authorities that will receive audit reports. The ES-C2M2 process should review who receives the audit reports. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Continuity of Operations: The organization continuity of operations plan should identify the assigned individuals to receive information and perform reporting obligations. The ES-C2M2 process should include a review of the list. The GRC requirements should be specified for the control systems.

Incident Response: The organization should identify who receives incident reports and who is responsible for coordinating emergency response. The ES-C2M2 process should include a review of the assigned personnel. The GRC requirements should be specified for the control systems.

Smart Grid Information System and Information Integrity: The organization should receive and disseminate security alerts, advisories, and directives. The ES-C2M2 process should include a review of the list of external organizations. The GRC requirement may need to be augmented for specific control systems or groups of control systems.

MIL2

Awareness and Training: The organization should establish and maintain contact with security groups to gather threat information. The ES-C2M2 process should include a review of the information sources for relevancy, for standard and emergency operations, and for sharing of sensitive or classified information. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Continuity of Operations: The organization continuity of operations plan should identify the assigned individuals to receive information and perform reporting obligations. The ES-C2M2 process should include a review of the list for relevancy. The GRC requirements should be specified for the control systems.

Incident Response: The organization should identify who is responsible for coordinating emergency response. The ES-C2M2 process should include a review of the assigned personnel. The GRC requirements should be specified for the control systems.

Smart Grid Information System and Information Integrity: The organization should receive and disseminate security alerts, advisories, and directives and implement procedures for sharing sensitive or classified information. The ES-C2M2 process should include a review of the list of external organizations for relevancy and for technical expertise. The GRC requirements should be specified for the control systems.

MIL3

Awareness and Training: The organization should establish and maintain contact with security groups for information sharing. The ES-C2M2 process should ensure that risk, timely exchange of information, and trust are addressed. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Audit and Accountability: The organization should identify the management authorities that will receive audit reports. The ES-C2M2 process should ensure that risk is considered when identifying information sharing parties. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Information Integrity: The organization should receive and disseminate security alerts, advisories, and directives. The ES-C2M2 process should include a review of the list of external organizations for shared interests. The GRC requirements should be specified for the control systems.

2. Management Activities

MIL1

No practice at MIL 1

MIL2

There are no applicable NISTIR 7628 security requirements.

MIL3

Information and Document Management: The organization should develop and implement policies and procedures for information and document management. The ES-C2M2 process should review the policies and procedures to ensure that applicable standards and/or guidelines are addressed. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Media Protection: The organization should develop and implement policies and procedures for media protection. The ES-C2M2 process should review the policies and procedures to ensure that applicable standards and/or guidelines are addressed. The GRC requirement should be defined at the organization level.

2.9 Event and Incident Response, Continuity of Operations

1. Detect Cybersecurity Events

MIL1

Incident Response: The organization should identify the recipient of cyber event reports. The ES-C2M2 process should include a review of the assigned personnel. The GRC requirements should be specified for the control systems.

Audit and Accountability: The organization should identify the management authorities that will receive audit reports related to cyber events. The ES-C2M2 process should include a review of the assigned personnel. The GRC requirements should be specified for the control systems.

MIL2

Continuity of Operations: The organization continuity of operations plan should specify the criteria for defining a cyber event. The ES-C2M2 process should include a review of the criteria. The GRC requirements should be specified for the control systems.

Incident Response: The organization should implement incident handling and incident monitoring capabilities. The ES-C2M2 process should review the capabilities to verify there is a repository of cyber event data. The GRC requirements should be specified for the control systems.

MIL3

Audit and Accountability: The organization should implement audit analysis and reporting capabilities. The ES-C2M2 process should review the criteria to support correlation analysis. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Incident Response: The organization should implement incident handling and incident response investigation and analysis. The ES-C2M2 process should review the criteria to ensure they support correlation analysis. The GRC requirements should be specified for the control systems.

2. Escalate Cybersecurity Events and Declare Incidents

MIL1

Smart Grid Information System and Information Integrity: The organization should implement information system monitoring for anomalous events and unauthorized activities. The ES-C2M2 process should include a review of the criteria for event escalation. SG.SI-4 is a CTR and may be applied to a subset of the control systems.

Incident Response: The organization should implement incident handling capabilities. The ES-C2M2 process should review the cyber security event analysis criteria. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

MIL2

Incident Response: The organization should implement incident handling capabilities. The ES-C2M2 process should review the criteria for escalating cyber events. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Information Integrity: The organization should implement information system monitoring for anomalous events and unauthorized activities. The ES-C2M2 process should include a review of the criteria for event escalation. SG.SI-4 is a CTR and may be applied to a subset of the control systems.

MIL3

Smart Grid Information System and Information Integrity: The organization should implement information system monitoring for anomalous events and unauthorized activities. The ES-C2M2 process should include a review of the criteria for event escalation to verify that it addresses risk. SG.SI-4 is a CTR and may be applied to a subset of the control systems.

Audit and Accountability: The organization should perform audit monitoring and analysis and generate audit reports. The ES-C2M2 process should include a review of the analysis criteria for determining trends and patterns. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Incident Response: The organization should implement incident handling capabilities. The ES-C2M2 process should review the analysis criteria for determining trends and patterns. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems. The GRC requirements should be specified for the control systems.

3. Respond to Incidents and Escalated Cybersecurity Events

MIL1

Continuity of Operations: The organization should identify roles and responsibilities related to cyber security events and include this information in the continuity of operations plan. The ES-C2M2 process should include a review of this documentation. The GRC requirements should be specified for the control systems.

Incident Response: The organization should assign incident response, incident handling, incident reporting, and coordination of emergency response roles and responsibilities. The ES-C2M2 process should include a review of the role and responsibility designations. The GRC requirements should be specified for the control systems.

Audit and Accountability: The organization should perform audit monitoring and analysis and generate audit reports. The ES-C2M2 process should include a review of the cyber security event reporting. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL2

Continuity of Operations: The organization should develop a continuity of operations plan control system recovery and reconstitution procedures. The ES-C2M2 process should include a review of this documentation to ensure all phase of the life cycle are addressed and IT and OT systems are included. The GRC requirements should be specified for the control systems.

Incident Response: The organization should develop incident response policies and procedures and incident response roles and responsibilities and conduct incident response training, testing, and exercises. The ES-C2M2 process should ensure the policies and procedures include IT and OT systems and address all phase of the system life cycle. The GRC requirements should be specified for the control systems.

Smart Grid Information System and Information Integrity: The organization should exercise/test the intrusion monitoring tools. The ES-C2M2 process should include a review of the exercise/test results. SG.SI-4 is a CTR and may be applied to a subset of the control system components.

MIL3

Security Assessment and Authorization: The organization should implement continuous improvement practices and lessons learned. The ES-C2M2 process should include a review of the revisions based on lessons learned. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Continuity of Operations: The organization should develop and update a continuity of operations plan. The ES-C2M2 process should include a review of the continuity of operations plan to verify that it is updated. The GRC requirements should be specified for the control systems.

Incident Response: The organization should develop incident response policies and procedures; assign incident response roles and responsibilities; develop incident handling, incident reporting, incident response investigation and analysis, corrective action, and coordination of emergency response procedures. The ES-C2M2 process should include a review of the procedures to ensure they are current, conform to applicable laws and regulations, and are updated at defined frequencies. The GRC requirements should be specified for the control systems.

Risk Management and Assessment: The organization should incorporate implement vulnerability assessment and awareness that incorporates lessons learned activities. The ES-C2M2 process should include an assessment of the process. The GRC requirements should be specified for the control systems.

4. Plan for Continuity

MIL1

Continuity of Operations: The organization should develop a continuity of operations plan, perform continuity of operations plan testing, and implement recovery and reconstitution. The ES-C2M2 process should include a review of the plans, testing results, and procedures for completeness. The GRC requirements should be specified for the control systems.

MIL2

Continuity of Operations: The organization should continuity of operations plan testing. The ES-C2M2 process should include a review of the testing results. The GRC requirements should be specified for the control systems.

MIL3

Continuity of Operations: The organization should update the continuity of operations plan. The ES-C2M2 process should ensure the plan is updated at regular intervals and that it addresses risk. The GRC requirements should be specified for the control systems.

5. Management Activities

MIL1

No practice at MIL 1

MIL2

Continuity of Operations: The organization should develop and update a continuity of operations plan, assign roles and responsibilities, and develop fail-safe response procedures. The ES-C2M2 process should review the plans and procedures. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems. SG.CP-11 is a CTR and may be applied to a subset of the control system components.

Incident Response: The organization should develop incident response policies and procedures, specify incident response roles and responsibilities, and coordination of emergency response procedures. The ES-C2M2 process should include a review of the documents and ensure that standards and guidelines are considered. The GRC requirements should be specified for the control systems.

MIL3

Incident Response: The organization should develop incident response policies and procedures and specify incident response roles and responsibilities. The ES-C2M2 process should include a review of the documents to ensure that policies, standards, and guidelines are considered. The GRC requirements should be specified for the control systems.

Continuity of Operations: The organization should assign continuity of operations roles and responsibilities. The ES-C2M2 process should include a review of this information. The GRC requirements should be specified for the control systems.

2.10 Supply Chain and External Dependencies Management

1. Identify Dependencies

MIL1

Access Control: The organization should identify critical external systems. The ES-C2M2 process should review the list of systems. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Information System and Services Acquisition: The organization should address supply chain vulnerabilities. The ES-C2M2 process should include an assessment of the supply chain process and the dependency criteria. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL2

Smart Grid Information System and Services Acquisition: The organization should address supply chain vulnerabilities. The ES-C2M2 process should include an assessment of the supply chain process and the dependency criteria. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

There are no applicable NISTIR 7628 security requirements.

2. Manage Dependency Risk

MIL1

Personnel Security: The organization should develop and enforce security requirements for contractors and third party personnel. The ES-C2M2 process should include an assessment of cyber security risk. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL2

Smart Grid Information System and Services Acquisition: The organization should include cyber security requirements in system acquisition contracts. The ES-C2M2 process should include a review of some contracts. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

Smart Grid Information System and Information Integrity: The organization should develop and implement monitoring techniques. The ES-C2M2 process should include a review of external dependencies management. SG.SI-4 is a CTR and may be applied to a subset of the system components.

Personnel Security: The organization should develop and enforce security requirements for contractors and third party personnel. The ES-C2M2 process should include an assessment of cyber security risk. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

3. Management Activities

MIL1

No practice at MIL 1

MIL2

There are no applicable NISTIR 7628 security requirements.

MIL3

Smart Grid Information System and Services Acquisition: The organization should develop acquisition security policies and procedures. The ES-C2M2 process should ensure that dependency risk is addressed and includes compliance requirements. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

2.11 Workforce Management

1. Assign Cybersecurity Responsibilities

MIL1

Awareness and Training: The organization should develop and provide security training to personnel. The ES-C2M2 process should include a review of the cyber security responsibilities included in the training. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Continuity of Operations: The organization should define continuity of operations roles and responsibilities and continuity of operations training materials. The ES-C2M2 should include a review of the responsibilities and ensure that these are assigned to individuals. The GRC requirements should be specified for the control systems.

Incident Response: The organization should develop and conduct incident response training. The ES-C2M2 process should include a review of the incident response cyber security responsibilities. The GRC requirements should be specified for the control systems.

Planning: The organization should define rules of behavior for personnel. The ES-C2M2 process should include a review of the cyber security responsibilities and ensure that these are assigned to individuals. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Security Program Management: The organization should identify management accountability, including roles and responsibilities for the cyber security program. The ES-C2M2 process should include a review of the responsibilities. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

Personnel Security: The organization should define roles and duties for employees, contractors, and third parties. The ES-C2M2 process should include a review of the cyber security responsibilities and ensure that these are assigned to individuals. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Communication Protection: The organization should define security roles and responsibilities for the control systems. The ES-C2M2 process should include a review of the cyber security responsibilities and ensure that these are documented and include external service providers. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL2

Awareness and Training: The organization should develop and provide security training to personnel. The ES-C2M2 process should include a review of the cyber security responsibilities included in the training and ensure that these include external service providers. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Continuity of Operations: The organization should define continuity of operations roles and responsibilities and continuity of operations training materials. The ES-C2M2 should include a review of the responsibilities and ensure that these include external service providers. The GRC requirements should be specified for the control systems.

Incident Response: The organization should develop and conduct incident response training. The ES-C2M2 process should include a review of the incident response cyber security responsibilities and ensure these include external service providers. The GRC requirements should be specified for the control systems.

Planning: The organization should define rules of behavior for personnel. The ES-C2M2 process should include a review of the cyber security responsibilities and ensure that these include external service providers. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Security Program Management: The organization should identify management accountability, including roles and responsibilities for the cyber security program. The ES-C2M2 process should include a review of the responsibilities and ensure that these include external service providers. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

Personnel Security: The organization should define roles and duties for employees, contractors, and third parties. The ES-C2M2 process should include a review of the cyber security responsibilities and ensure that these are documented and include external service providers. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Communication Protection: The organization should define security roles and responsibilities for the control systems. The ES-C2M2 process should include a review of the cyber security responsibilities and ensure that these are documented and include external service providers. The GRC requirements should be specified for the control systems.

MIL3

There are no applicable NISTIR 7628 security requirements.

2. Control the Workforce Life Cycle

MIL1

Personnel Security: The organization performs personnel screening and develop personnel termination procedures. The ES-C2M2 process should include a review of the screening process to ensure consistency with organization-defined guidance and that personnel termination includes both physical and logical access. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL2

Personnel Security: The organization should perform personnel screening and develop personnel transfer procedures. The ES-C2M2 process should include a review of the screening process to ensure consistency with organization-defined guidance and that personnel termination includes both physical and logical access. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

Personnel Security: The organization should develop personnel security policies and procedures, position categorization, personnel screening criteria, contractor and third party personnel requirements, personnel accountability processes, and personnel duties and terms and conditions of employment. The ES-C2M2 process should include a review of the policies and procedures. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

3. Develop Cybersecurity Workforce

MIL1

Awareness and Training: The organization should develop and perform security awareness, security training, and planning process training. The ES-C2M2 process should include a review of the awareness and training materials and ensure that the training material is available to those with cyber security responsibilities. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

MIL2

Awareness and Training: The organization should develop and perform security awareness, security training, and planning process training. The ES-C2M2 process should include a review of the awareness and training materials and identify any gaps. Also, training should be conducted prior to system access. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

Personnel Security: The organization should develop personnel security policies and procedures. The ES-C2M2 process should include a review of the policies and procedures. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Awareness and Training: The organization should develop and perform security training and planning process training. The ES-C2M2 process should include a review of the training materials and ensure they are aligned with organization objectives and are revised, as appropriate. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

4. Increase Cybersecurity Awareness

MIL1

Awareness and Training: The organization should develop and perform security awareness. The ES-C2M2 process should include a review of the awareness materials. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL2

There are no applicable NISTIR 7628 security requirements.

MIL3

There are no applicable NISTIR 7628 security requirements.

5. Management Activities

MIL1

No practice at MIL 1

MIL2

Awareness and Training: The organization should maintain security awareness and training records and develop and implement awareness and training procedures. The ES-C2M2 process should include a review of the records and the procedures. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Personnel Security: The organization should define personnel roles and responsibilities. The ES-C2M2 process should include identification of the appropriate stakeholders. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

There are no applicable NISTIR 7628 security requirements.

2.12 Cybersecurity Program Management

1. Establish Cybersecurity Program Strategy

MIL1

There are no applicable NISTIR 7628 security requirements.

MIL2

There are no applicable NISTIR 7628 security requirements.

MIL3

Security Assessment and Authorization: The organization should perform security assessments and implement continuous improvement and continuous monitoring. The ES-C2M2 process should ensure the assessments and processes are updated to reflect changes in the operational and threat environments. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Planning: The organization should develop security plans for the control systems. The ES-C2M2 process should include an assessment of the plans to ensure they address changes in the environment. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

2. Sponsor Cybersecurity Program

MIL1

Security Program Management: The organization should appoint a senior management authority to develop, implement, and maintain the cyber security program. The ES-C2M2 process should include a review of these assigned responsibilities. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

MIL2

Security Program Management: The organization should develop security program policies and procedures. The ES-C2M2 process should include a review of management responsibility. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

MIL3

Security Program Management: The organization should develop security program policies and procedures. The ES-C2M2 process should include a review of the policies and procedures to ensure they address applicable regulations. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

3. Establish and Maintain Cybersecurity Architecture

MIL1

Access Control: The organization should implement information flow enforcement and control system access restrictions. The ES-C2M2 process should include a review of the system architecture. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems. SG.AC-19 is a CTR. SG.AC-5 is a UTR. These may be applied to a subset of the control system components. (Note: SG.AC-5 is a significant technical control and not typically implemented in control systems.)

Smart Grid Information System and Communication Protection: The organization should implement boundary protection. The ES-C2M2 process should include a review of the system architecture. SG.SC-7 is a UTR and may be applied to a subset of the control system components.

MIL2

Access Control: The organization should implement information flow enforcement and control system access restrictions. The ES-C2M2 process should include a review of the cyber security architecture and the implemented segmentation and isolation. SG.AC-19 is a CTR. SG.AC-5 is a UTR. These controls may be applied to a subset of the control system components. (Note: SG.AC-5 is a significant technical control and not typically implemented in control systems.)

Continuity of Operations: The organization should identify alternate storage sites and alternate telecommunication services. The ES-C2M2 process should include a review of the alternate storage site plan, the transfer of backup information to the alternate storage site, and the alternate telecommunication plans. The GRC requirements may need to be tailored/augmented for specific control systems or groups of control systems.

Physical and Environmental Security: The organization should establish an alternate work site, as appropriate. The ES-C2M2 process should include a review the alternate work site procedures. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Smart Grid Information System and Communication Protection: The organization should implement security function isolation, denial-of-service protection, boundary protection, system connections, and message authenticity. The ES-C2M2 process should include a review of the implemented controls. SG.SC-3, SG.SC-5, and SG.SC-7 are UTRs. SG.SC-18 and SG.SC-20 are CTRs. These controls may be applied to a subset of the control system components.

MIL3

Access Control: The organization should implement information flow enforcement and control system access restrictions. The ES-C2M2 process should include a review of the system architecture to ensure it is updated at a defined frequency. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems. SG.AC-19 is a CTR. SG.AC-5 is a UTR. These controls may be applied to a subset of the control system components. (Note: SG.AC-5 is a significant technical control and not typically implemented in control systems.)

Smart Grid Information System and Communication Protection: The organization should implement boundary protection. The ES-C2M2 process should include a review of the system architecture to ensure it is updated at a defined frequency. SG.SC-7 is a UTR and may be applied to a subset of the control system components.

4. Perform Secure Software Development

MIL1

No practice at MIL 1

MIL2

There are no applicable NISTIR 7628 security requirements.

MIL3

There are no applicable NISTIR 7628 security requirements.

5. Management Activities

MIL1

No practice at MIL 1

MIL2

Security Program Management: The organization should develop and disseminate a security program plan. The ES-C2M2 process should include a review of the program plan and the identification of stakeholders. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

MIL3

Planning: The organization should plan and coordinate security-related activities before executing the activities. The ES-C2M2 process should include a review of the plans. The GRC requirement may need to be tailored/augmented for specific control systems or groups of control systems.

Security Program Management: The organization should develop and disseminate security program policies and procedures and a security program plan. The ES-C2M2 process should include a review of the policies, procedure, and plan to ensure that organization polices/directives are incorporated and the documents are periodically reviewed and update. The GRC security program management controls are typically implemented at the organization level and not in individual systems. As required, tailoring guidance can be applied to the security program management controls for specific control systems or groups of control systems.

3

NISTIR 7628 LOGICAL INTERFACE DIAGRAMS

Included below are the 22 logical interface category (LIC) diagrams extracted from the NISTIR 7628, the associated UTRs and ES-C2M2 practices. Below the diagrams is a list of the ES-C2M2 practices allocated to each NISTIR 7628 requirement. Each ES-C2M2 practice is tailored for the specific NISTIR 7628 requirements.

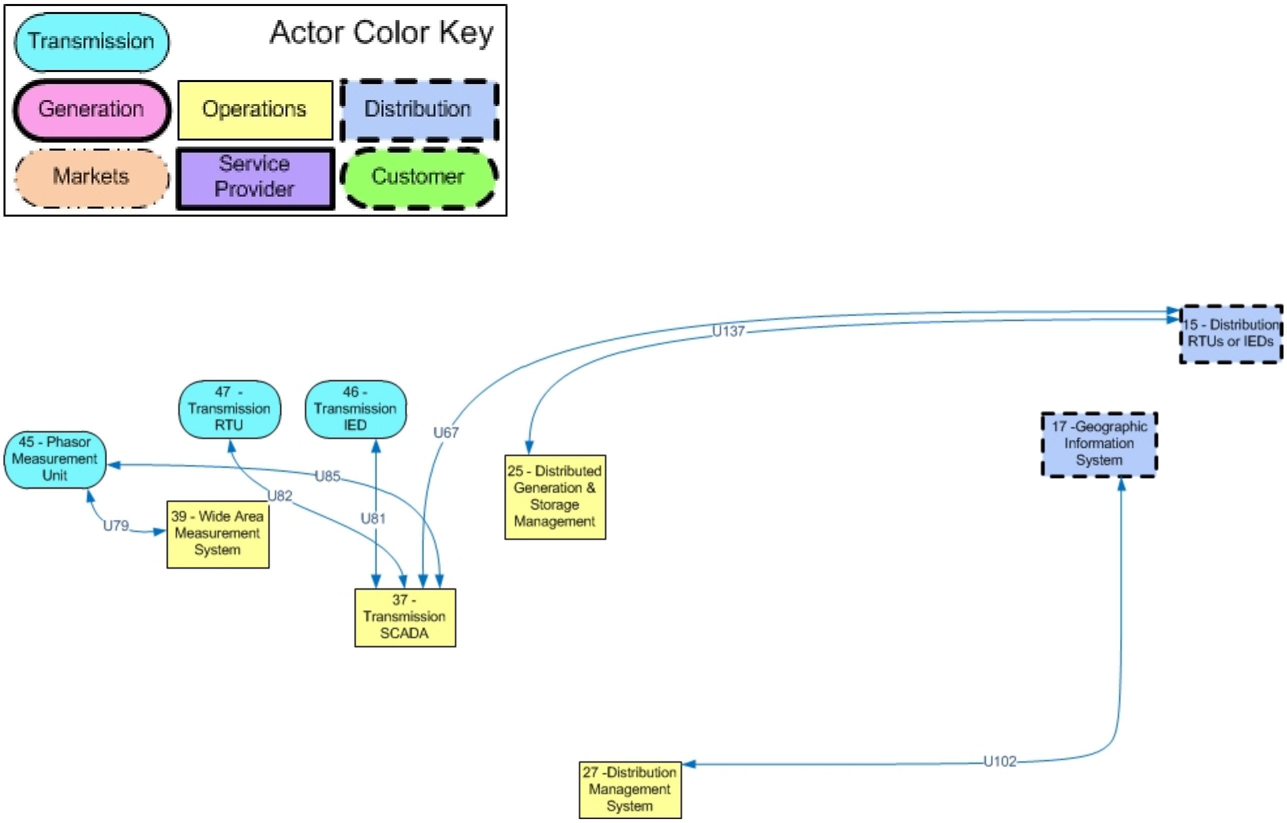

Actor Color Key
Transmission
Generation
Operations
Distribution
Markets
Service Provider
Customer
15 - Distribution RTUs or IEDs
U137
47 - Transmission RTU
46 - Transmission IED
U67
17 -Geographic Information System
45 - Phasor Measurement Unit
U85
25 - Distributed Generation & Storage Management
U82
U79
39 - Wide Area Measurement System
U81
37 - Transmission SCADA
27 -Distribution Management System
U102

Figure 3-1
Logical Interface Categories 1-4: Interface Between Control Systems and Equipment With/Without High Availability, and With/Without Compute and/or Bandwidth Constraints

[The diagram was extracted from the NISTIR 7628]

Unique Technique Requirements:

- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.

- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-5: Denial-of-Service Protection:
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

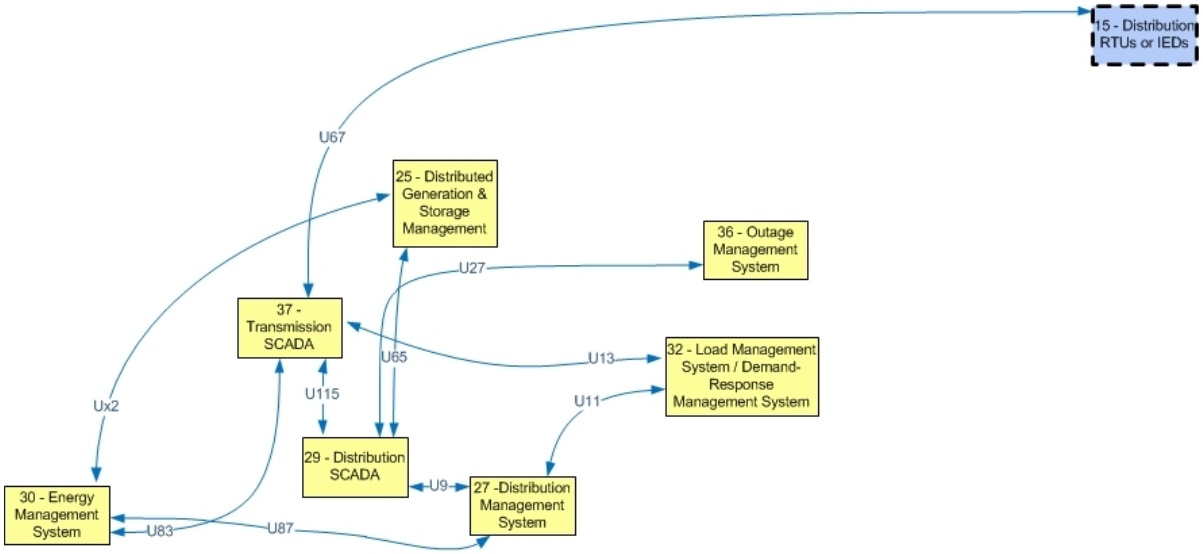

15 - Distribution RTUs or IEDs
U67
25 - Distributed Generation & Storage Management
36 - Outage Management System
U27
37 - Transmission SCADA
U65
U13
32 - Load Management System / Demand-Response Management System
Ux2
U115
U11
29 - Distribution SCADA
U9
27 -Distribution Management System
30 - Energy Management System
U83
U87

Figure 3-2
Logical Interface Category 5: Interface Between Control Systems within the Same Organization

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-14: Permitted Actions with Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.SC-5: Denial-of-Service Protection

- The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.

- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

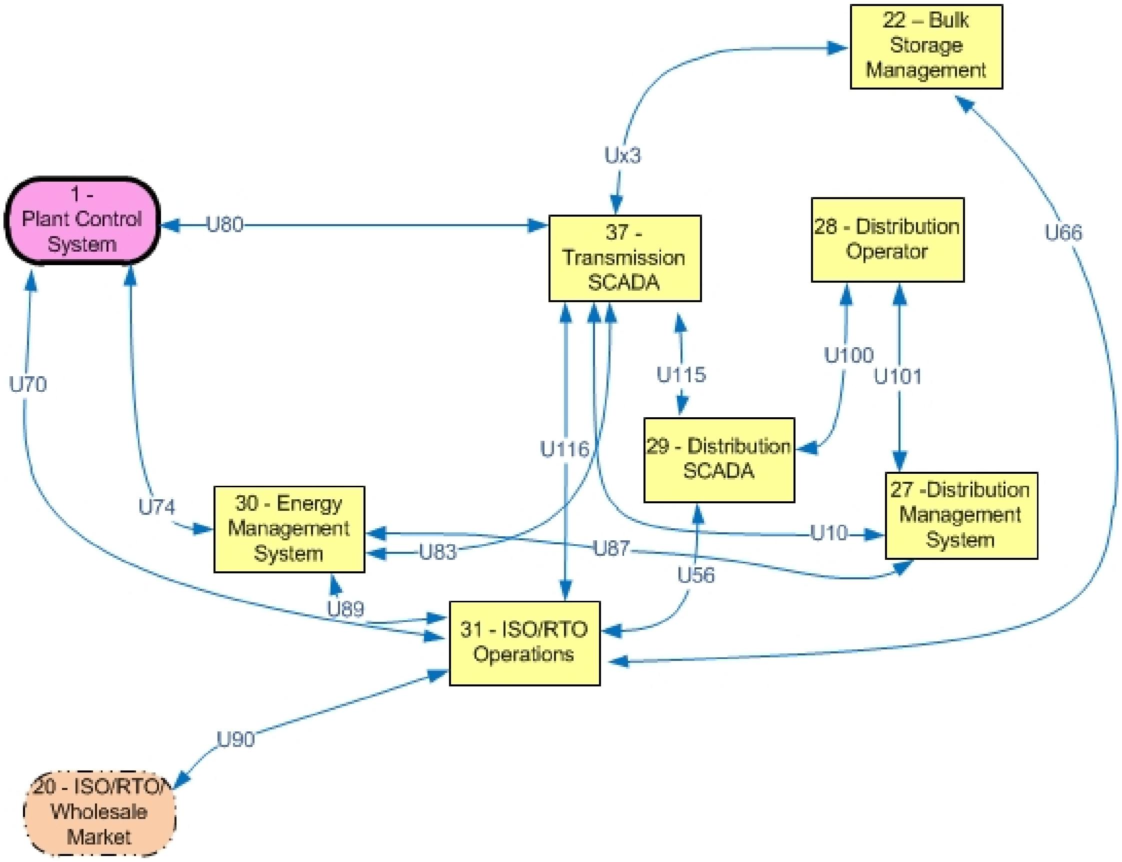

22 – Bulk Storage Management
Ux3
1 - Plant Control System
U80
37 - Transmission SCADA
28 - Distribution Operator
U66
U70
U115
U100
U101
U116
29 - Distribution SCADA
U74
30 - Energy Management System
27 -Distribution Management System
U10
U83
U87
U56
U89
31 - ISO/RTO Operations
U90
20 - ISO/RTO Wholesale Market

Figure 3-3
Logical Interface Category 6: Interface Between Control Systems in Different Organizations

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-14: Permitted Actions with Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.SC-5: Denial-of-Service Protection

  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

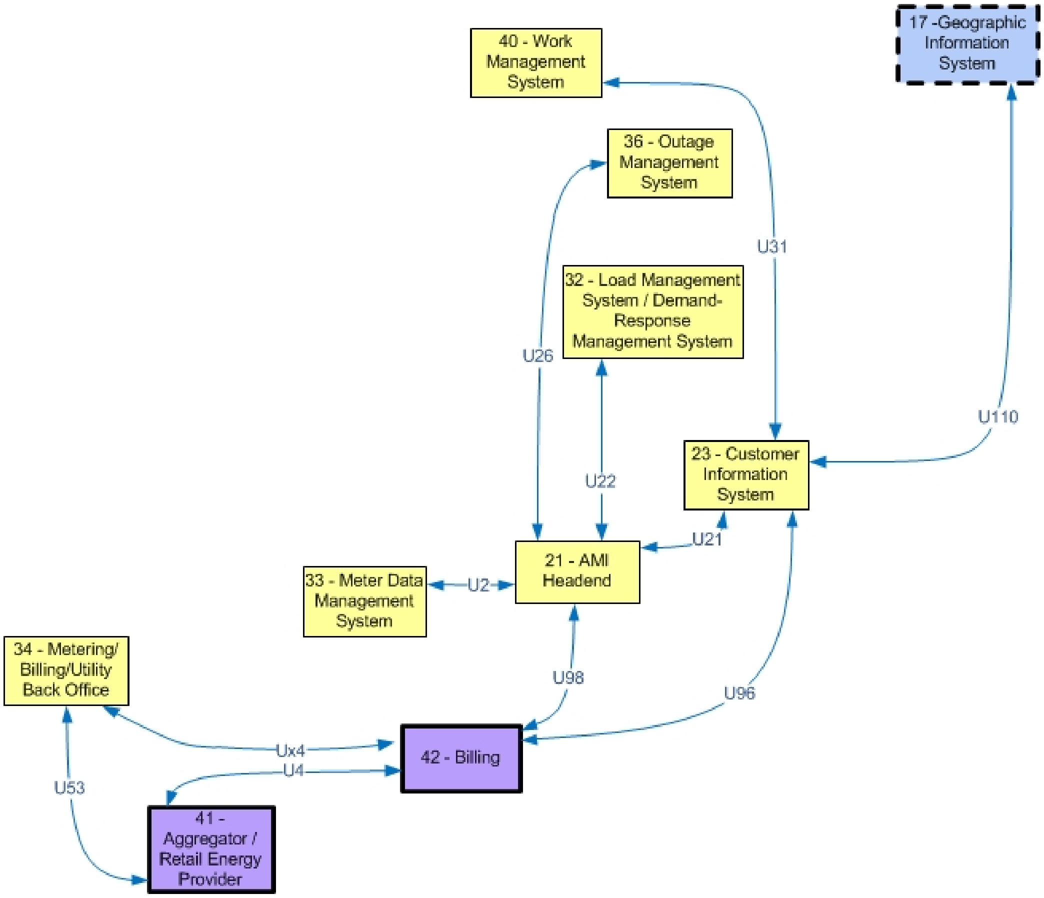

40 - Work Management System
17 -Geographic Information System
36 - Outage Management System
U31
32 - Load Management System / Demand-Response Management System
U26
U110
23 - Customer Information System
U22
U21
21 - AMI Headend
33 - Meter Data Management System
U2
34 - Metering/ Billing/Utility Back Office
U98
U96
Ux4
U4
42 - Billing
U53
41 - Aggregator / Retail Energy Provider

Figure 3-4
Logical Interface Category 7: Interface Between Back Office Systems under Common Management Authority

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-12: Session Lock
  - There are no associated ES-C2M2 practices.
- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.

- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-26: Confidentiality of Information at Rest
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

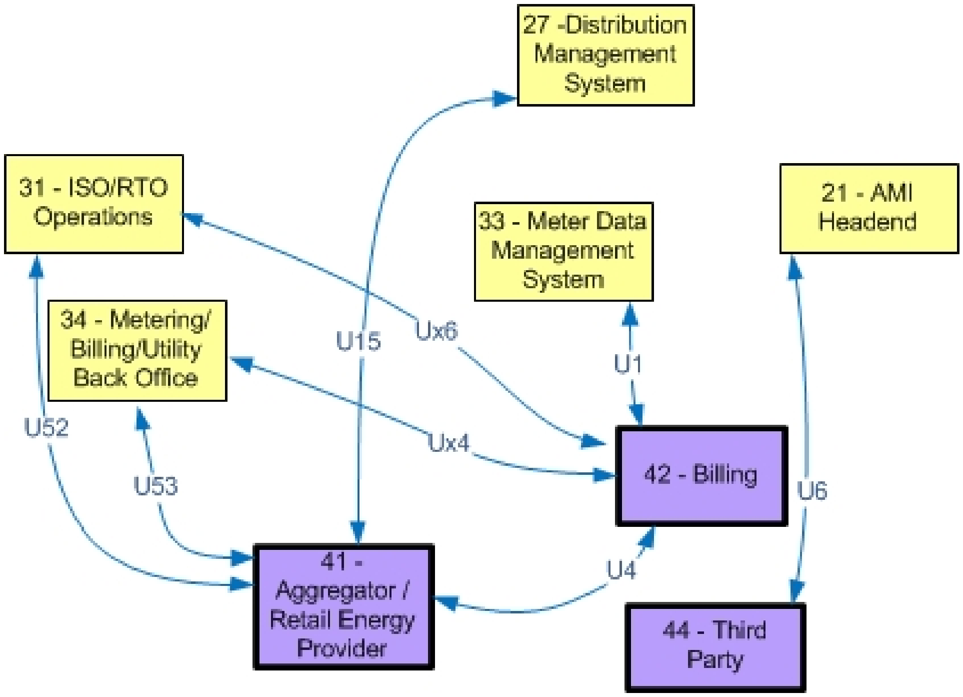

27 -Distribution Management System
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
34 - Metering/ Billing/Utility Back Office
U15
Ux6
U1
U52
Ux4
42 - Billing
U53
U6
U4
41 - Aggregator / Retail Energy Provider
44 - Third Party

Figure 3-5
Logical Interface Category 8: Interface Between Back Office Systems under Common Management Authority

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements

- SG.AC-12: Session Lock
  - There are no associated ES-C2M2 practices.
- SG.AC-14: Permitted Actions without Identification or Authentication

- The associated ES-C2M2 practice is IAM-2a.

- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-5: Denial-of-Service Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-6: Resource Priority
  - The associated ES-C2M2 practices are ACM-1b, ACM-1c, and ACM-1d.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-26: Confidentiality of Information at Rest
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

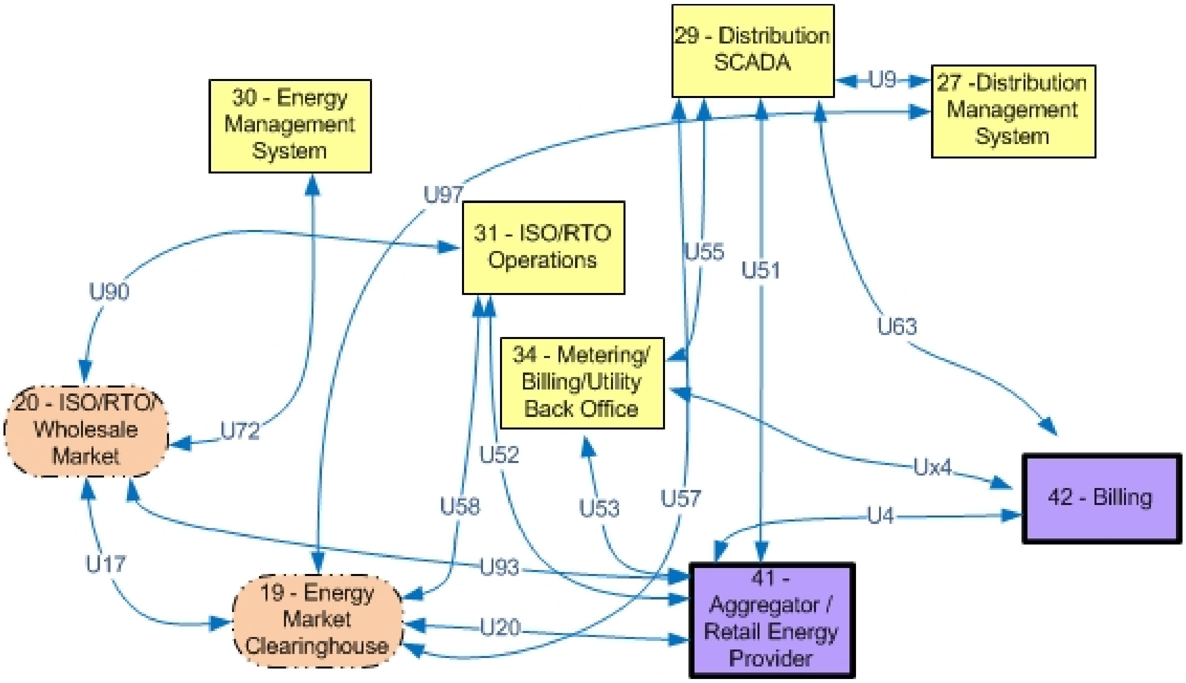

29 - Distribution SCADA
U9
27 -Distribution Management System
30 - Energy Management System
U97
31 - ISO/RTO Operations
U55
U51
U90
U63
34 - Metering/ Billing/Utility Back Office
20 - ISO/RTO/ Wholesale Market
U72
U52
Ux4
42 - Billing
U58
U53
U57
U4
U17
U93
41 - Aggregator / Retail Energy Provider
19 - Energy Market Clearinghouse
U20

Figure 3-6
Logical Interface Category 9: Interface with B2B Connections between Systems Usually Involving Financial or Market Transactions

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements

- SG.AC-12: Session Lock
  - There are no associated ES-C2M2 practices.
- SG.AC-13: Remote Session Termination
- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AC-15: Remote Access
  - The associated ES-C2M2 practices are: IAM-2a, IAM-2b, IAM-2c, IAM-2e, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, and SA-2i.
- SG.AU-16: Non-Repudiation
  - There are no associated ES-C2M2 practices.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.SC-5: Denial-of-Service Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.

- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-9: Communication Confidentiality
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

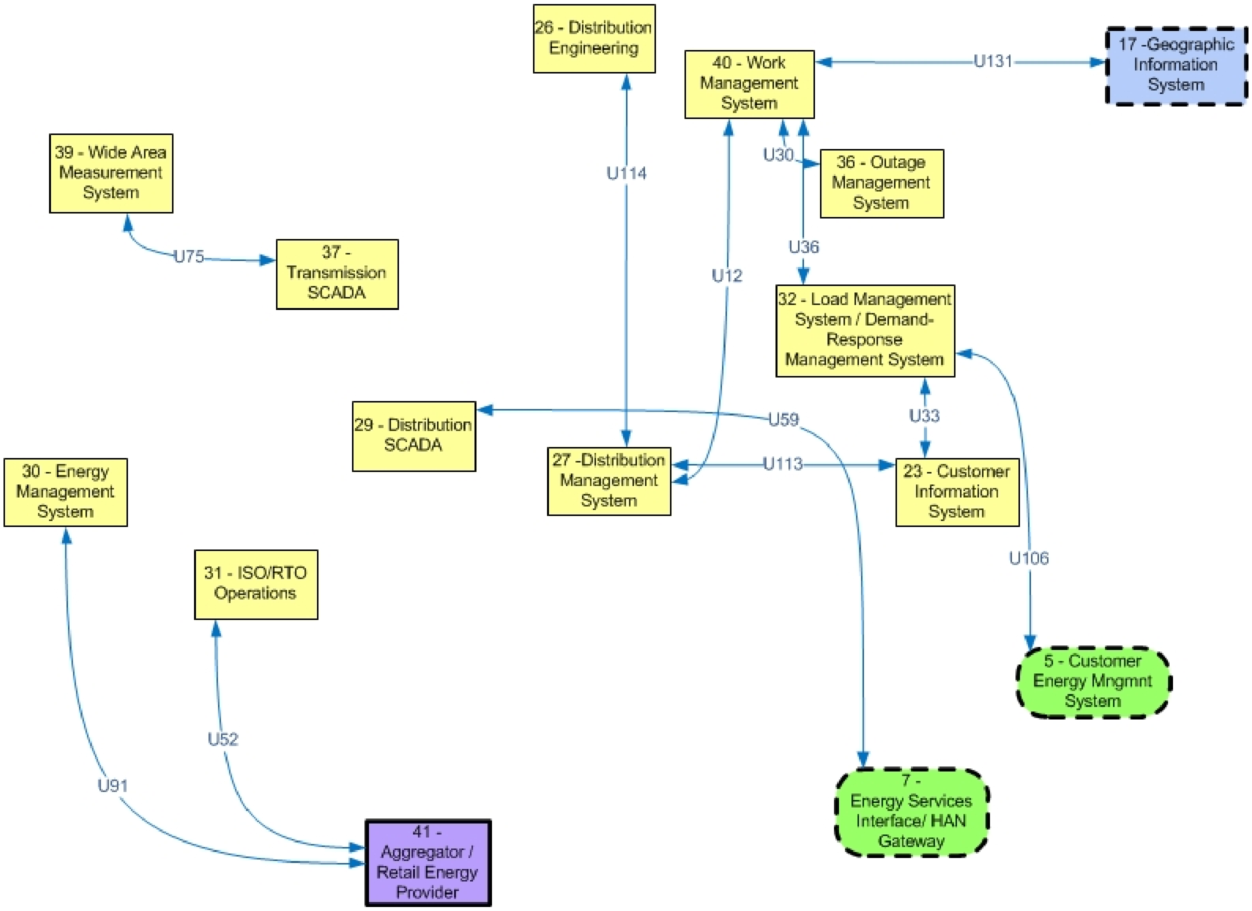

26 - Distribution Engineering
40 - Work Management System
U131
17 -Geographic Information System
39 - Wide Area Measurement System
U114
U30
36 - Outage Management System
U75
37 - Transmission SCADA
U36
U12
32 - Load Management System / Demand-Response Management System
U33
29 - Distribution SCADA
U59
30 - Energy Management System
27 -Distribution Management System
U113
23 - Customer Information System
U106
31 - ISO/RTO Operations
5 - Customer Energy Mngmnt System
U52
U91
7 - Energy Services Interface/ HAN Gateway
41 - Aggregator / Retail Energy Provider

Figure 3-7
Logical Interface Category 10: Interface Between Control Systems and Non-Control/ Corporate Systems

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.SC-5: Denial-of-Service Protection

  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.

- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-26: Confidentiality of Information at Rest
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

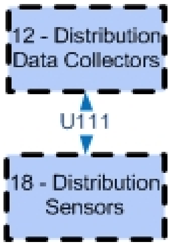


Figure 3-8
Logical Interface Category 11: Interface Between Sensors and Sensor Networks for Measuring Environmental Parameters, Usually Simple Sensor Devices with Possibly Analog Measurements

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirement:

- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.

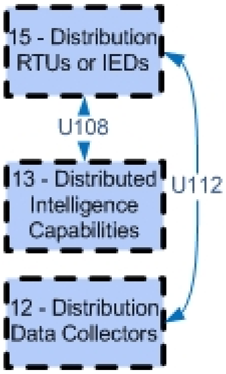

15 - Distribution RTUs or IEDs
U108
13 - Distributed Intelligence Capabilities
U112
12 - Distribution Data Collectors

Figure 3-9
Logical Interface Category 12: Interface Between Sensor Networks and Control Systems

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.

- SG.SC-5: Denial-of-Service Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

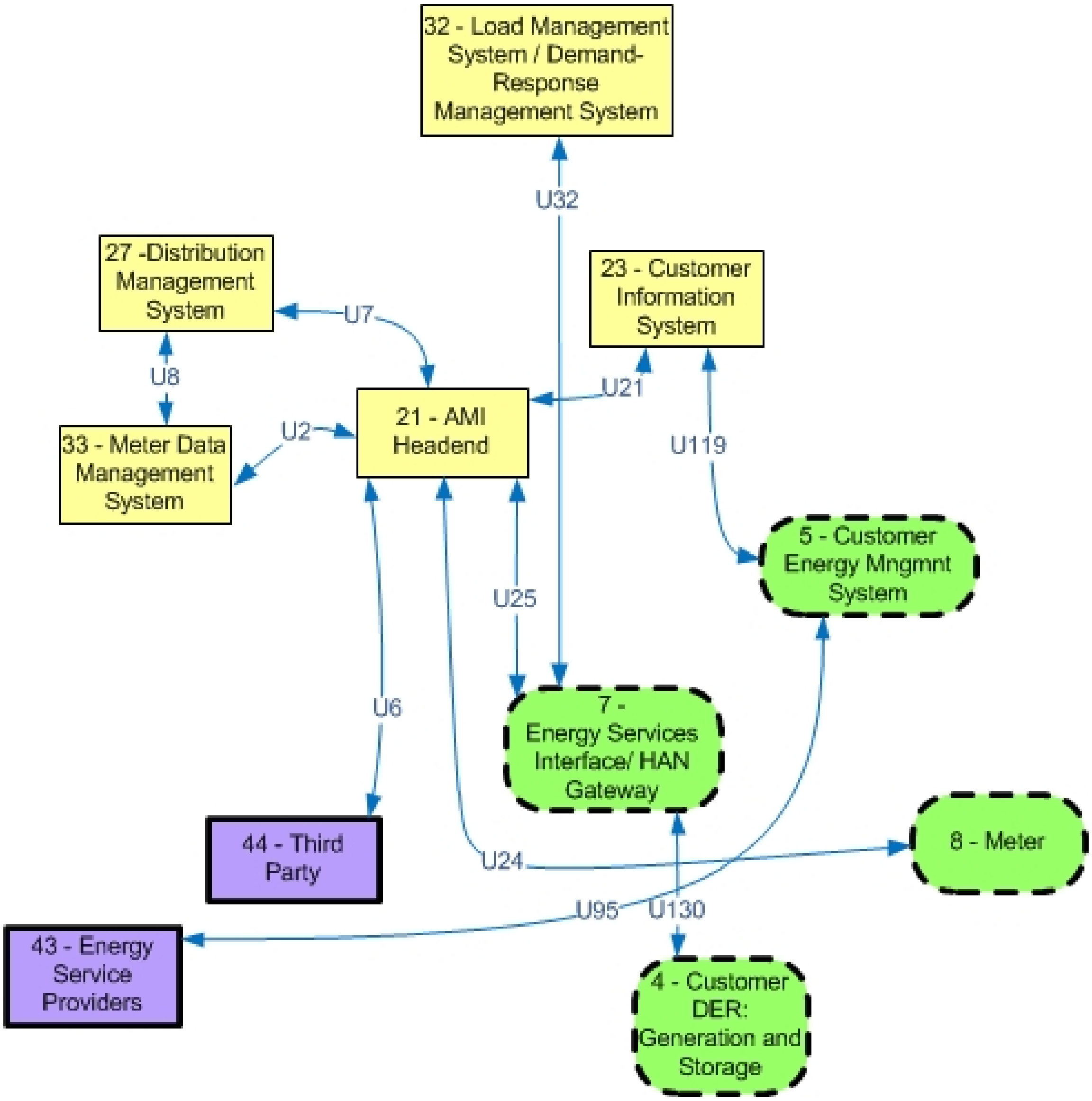

32 - Load Management System / Demand-Response Management System
U32
27 -Distribution Management System
U7
23 - Customer Information System
U8
U21
33 - Meter Data Management System
U2
21 - AMI Headend
U119
5 - Customer Energy Mngmnt System
U25
U6
7 - Energy Services Interface/ HAN Gateway
44 - Third Party
U24
8 - Meter
U95
U130
43 - Energy Service Providers
4 - Customer DER: Generation and Storage

Figure 3-10
Logical Interface Category 13: Interface between Systems that use the AMI Network

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AU-16: Non-Repudiation
  - There are no associated ES-C2M2 practices.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-9: Communication Confidentiality
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-26: Confidentiality of Information at Rest
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

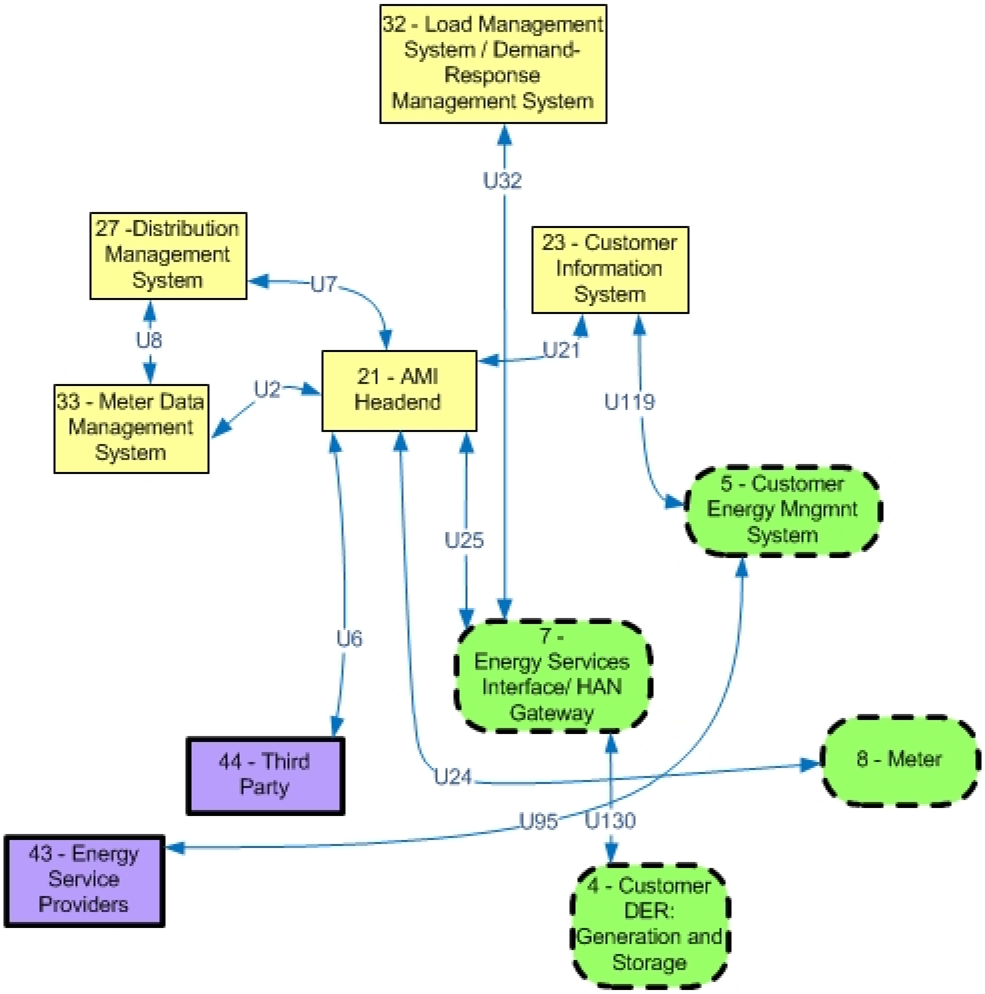

32 - Load Management System / Demand-Response Management System
U32
27 -Distribution Management System
U7
23 - Customer Information System
U8
U21
21 - AMI Headend
33 - Meter Data Management System
U2
U119
5 - Customer Energy Mngmnt System
U25
U6
7 - Energy Services Interface/ HAN Gateway
8 - Meter
44 - Third Party
U24
U95
U130
43 - Energy Service Providers
4 - Customer DER: Generation and Storage

Figure 3-11
Logical Interface Category 14: Interface between Systems that use the AMI Network for Functions That Require High Availability

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AU-16: Non-Repudiation
  - There are no associated ES-C2M2 practices.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.

- SG.SC-5: Denial-of-Service Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-9: Communication Confidentiality
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-26: Confidentiality of Information at Rest
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

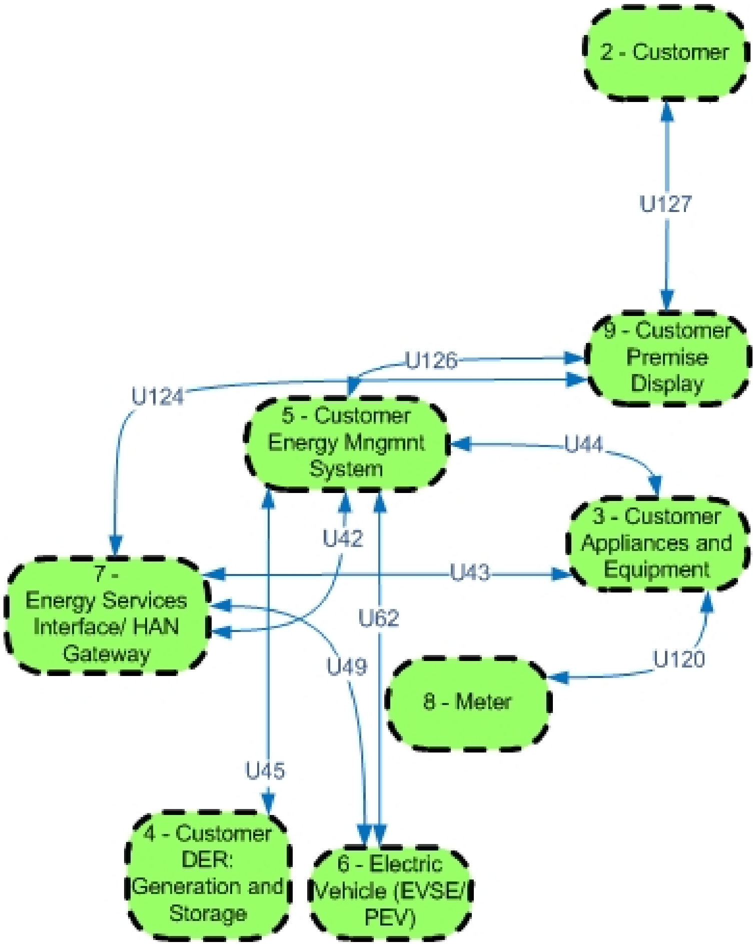
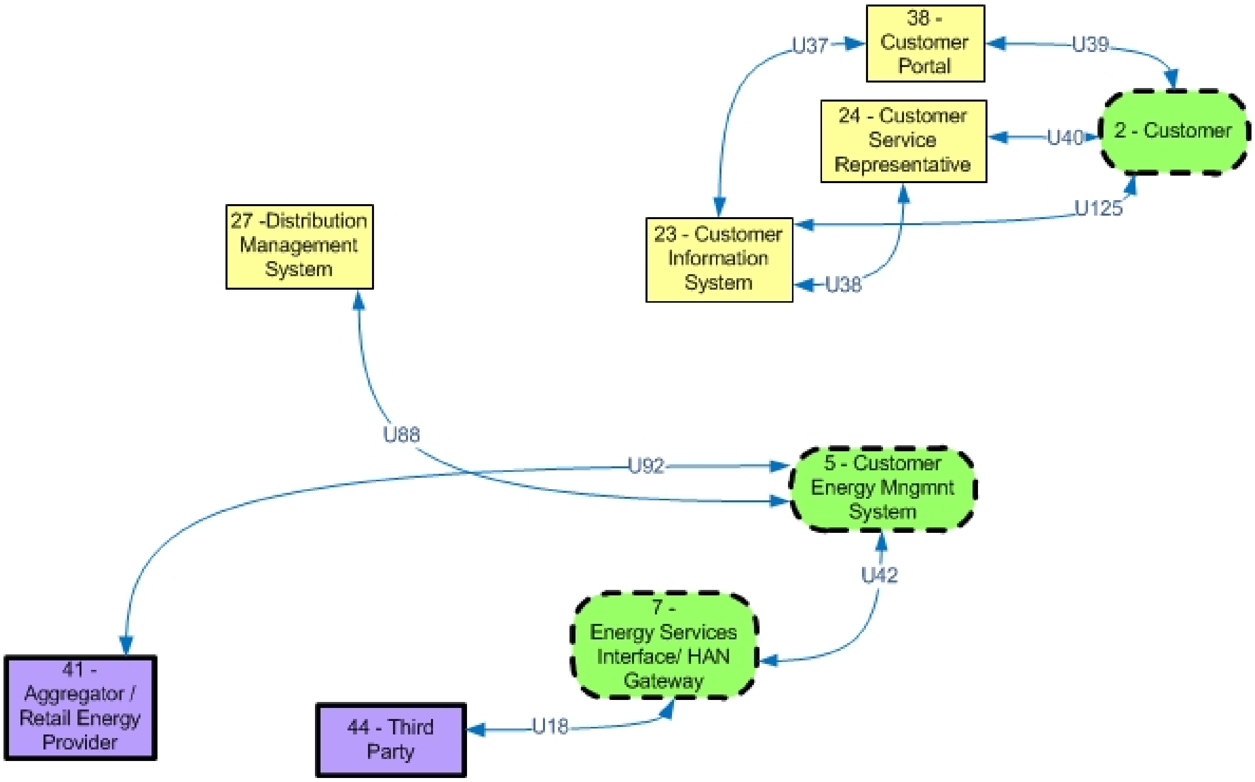

2 - Customer
U127
9 - Customer Premise Display
U126
U124
5 - Customer Energy Mngmnt System
U44
3 - Customer Appliances and Equipment
U42
U43
7 - Energy Services Interface/ HAN Gateway
U62
U49
U120
8 - Meter
U45
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/ PEV)

Figure 3-12
Logical Interface Category 15: Interface Between Systems That Use Customer (Residential, Commercial, and Industrial) Site Networks Such as HANs and BANs

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-12: Session Lock
  - There are no associated ES-C2M2 practices.
- SG.AC-13: Remote Session Termination
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AC-15: Remote Access
  - The associated ES-C2M2 practices are: IAM-2a, IAM-2b, IAM-2c, IAM-2e, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, and SA-2i
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-5: Denial-of-Service Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-9: Communication Confidentiality
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-26: Confidentiality of Information at Rest
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.



38 - Customer Portal
U37
U39
24 - Customer Service Representative
U40
2 - Customer
U125
27 -Distribution Management System
23 - Customer Information System
U38
U88
U92
5 - Customer Energy Mngmnt System
U42
7 - Energy Services Interface/ HAN Gateway
41 - Aggregator / Retail Energy Provider
44 - Third Party
U18

Figure 3-13
Logical Interface Category 16: Interface Between External Systems and the Customer Site

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AU-16: Non-Repudiation
  - There are no associated ES-C2M2 practices.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-5: Denial-of-Service Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
  - SG.SC-7: Boundary Protection The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity

  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.

- SG.SC-9: Communication Confidentiality
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-26: Confidentiality of Information at Rest
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

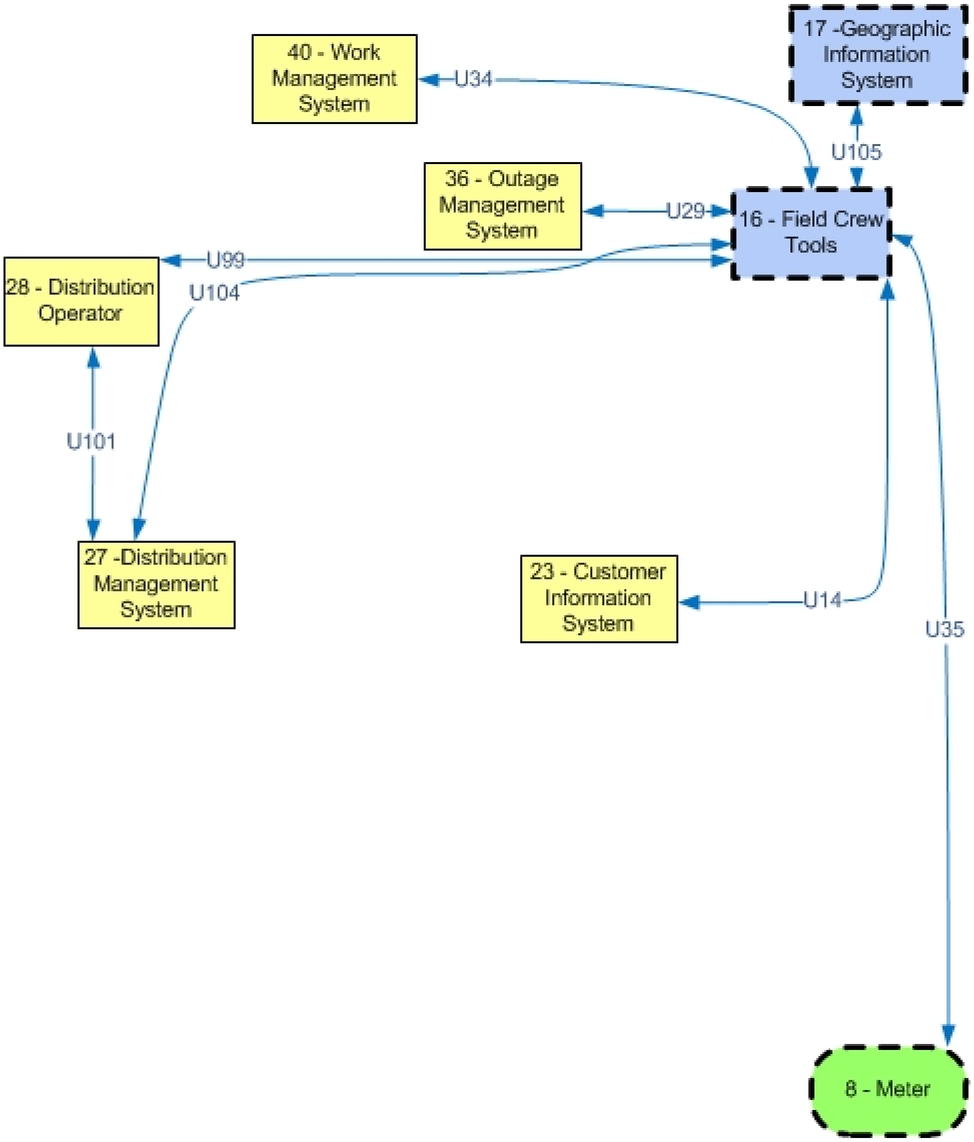

17 -Geographic Information System
40 - Work Management System
U34
U105
36 - Outage Management System
U29
16 - Field Crew Tools
28 - Distribution Operator
U99
U104
U101
27 -Distribution Management System
23 - Customer Information System
U14
U35
8 - Meter

Figure 3-14
Logical Interface Category 17: Interface Between Systems and Mobile Field Crew Laptops/Equipment

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-12: Session Lock
  - There are no associated ES-C2M2 practices.
- SG.AC-13: Remote Session Termination
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

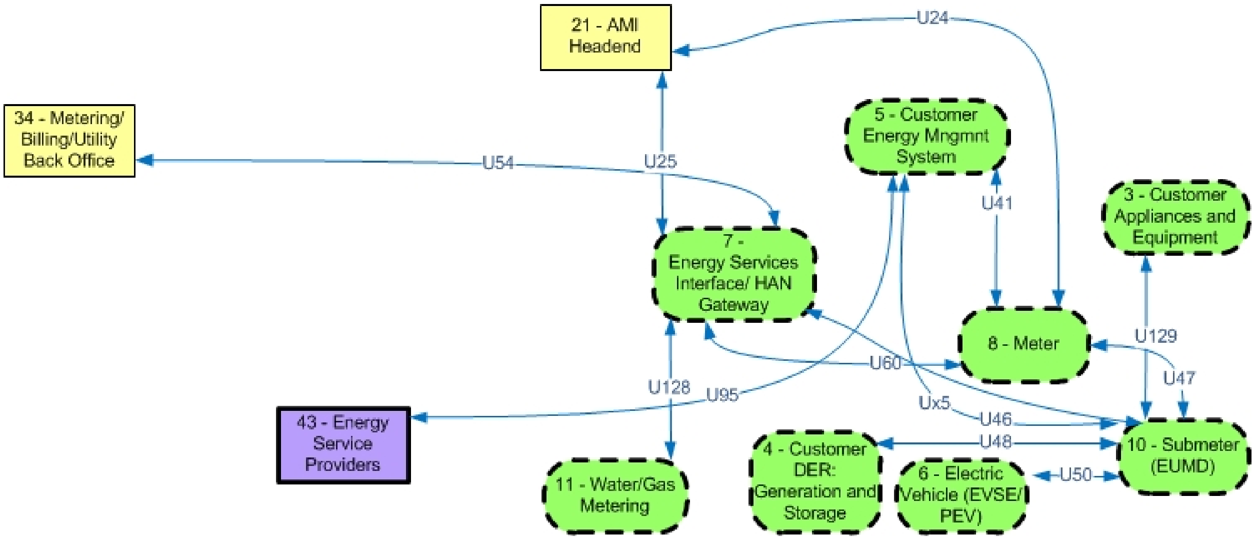

21 - AMI Headend
U24
34 - Metering/ Billing/Utility Back Office
U54
U25
5 - Customer Energy Mngmnt System
U41
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
8 - Meter
U129
U47
U60
U128
U95
Ux5
U46
U48
43 - Energy Service Providers
11 - Water/Gas Metering
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/ PEV)
U50
10 - Submeter (EUMD)

Figure 3-15
Logical Interface Category 18: Interface Between Metering Equipment

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.IA-4: User Identification and Authentication

  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-9: Communication Confidentiality
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-26: Confidentiality of Information at Rest
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

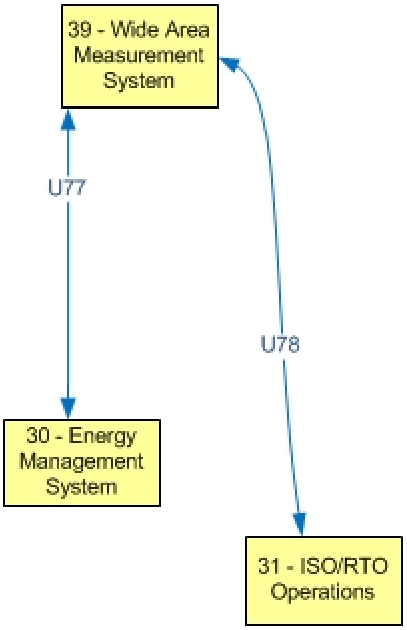

39 - Wide Area Measurement System
U77
U78
30 - Energy Management System
31 - ISO/RTO Operations

Figure 3-16
Logical Interface Category 19: Interface Between Operations Decision Support Systems

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-13: Remote Session Termination
  - The associated ES-C2M2 practice is IAM-2a.
- SG.IA-5: Device Identification and Authentication

- The associated ES-C2M2 practices are IAM-1a and IAM-1b.

- SG.SC-5: Denial-of-Service Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-9: Communication Confidentiality
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

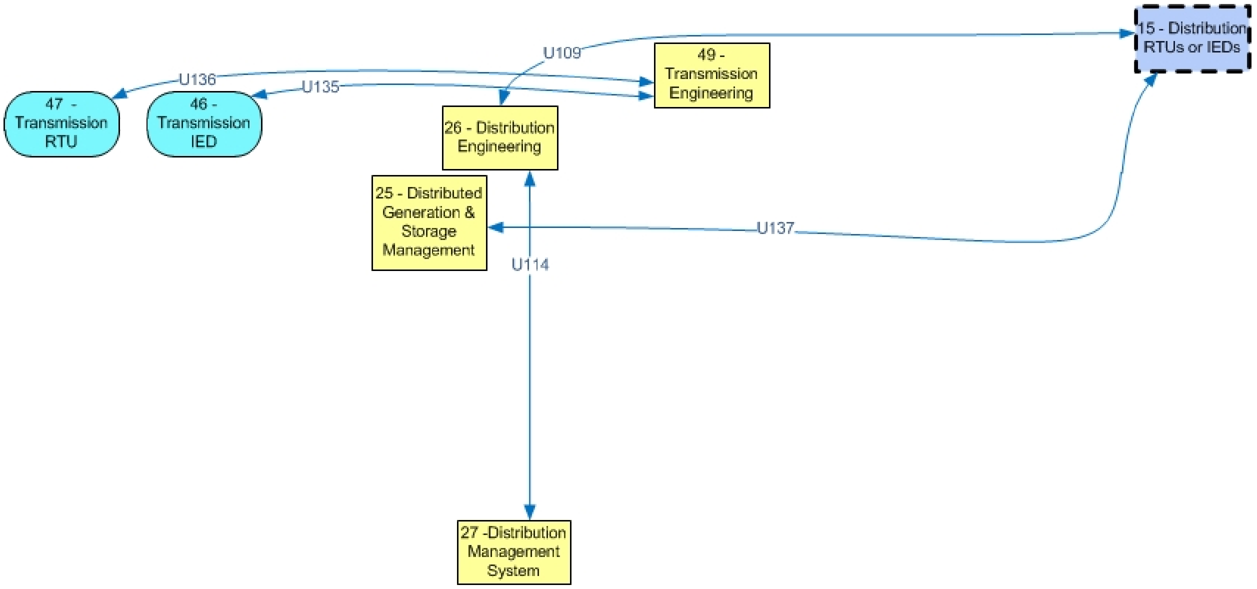

15 - Distribution RTUs or IEDs
U109
49 - Transmission Engineering
U136
U135
47 - Transmission RTU
46 - Transmission IED
26 - Distribution Engineering
25 - Distributed Generation & Storage Management
U137
U114
27 -Distribution Management System

Figure 3-17
Logical Interface Category 20: Interface Between Engineering/Maintenance Systems and Control Equipment

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AC-15: Remote Access
  - The associated ES-C2M2 practices are: IAM-2a, IAM-2b, IAM-2c, IAM-2e, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, and SA-2i
- SG.AU-16: Non-Repudiation
  - There are no associated ES-C2M2 practices.

- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

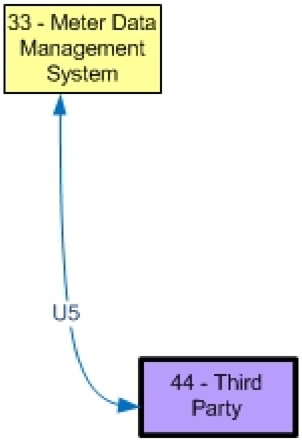


Figure 3-18
Logical Interface Category 21: Interface Between Control Systems and Their Vendors for Standard Maintenance and Service

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-12: Session Lock
  - There are no associated ES-C2M2 practices.
- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AC-15: Remote Access
  - The associated ES-C2M2 practices are: IAM-2a, IAM-2b, IAM-2c, IAM-2e, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, and SA-2i
- SG.AU-16: Non-Repudiation

  - There are no associated ES-C2M2 practices.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

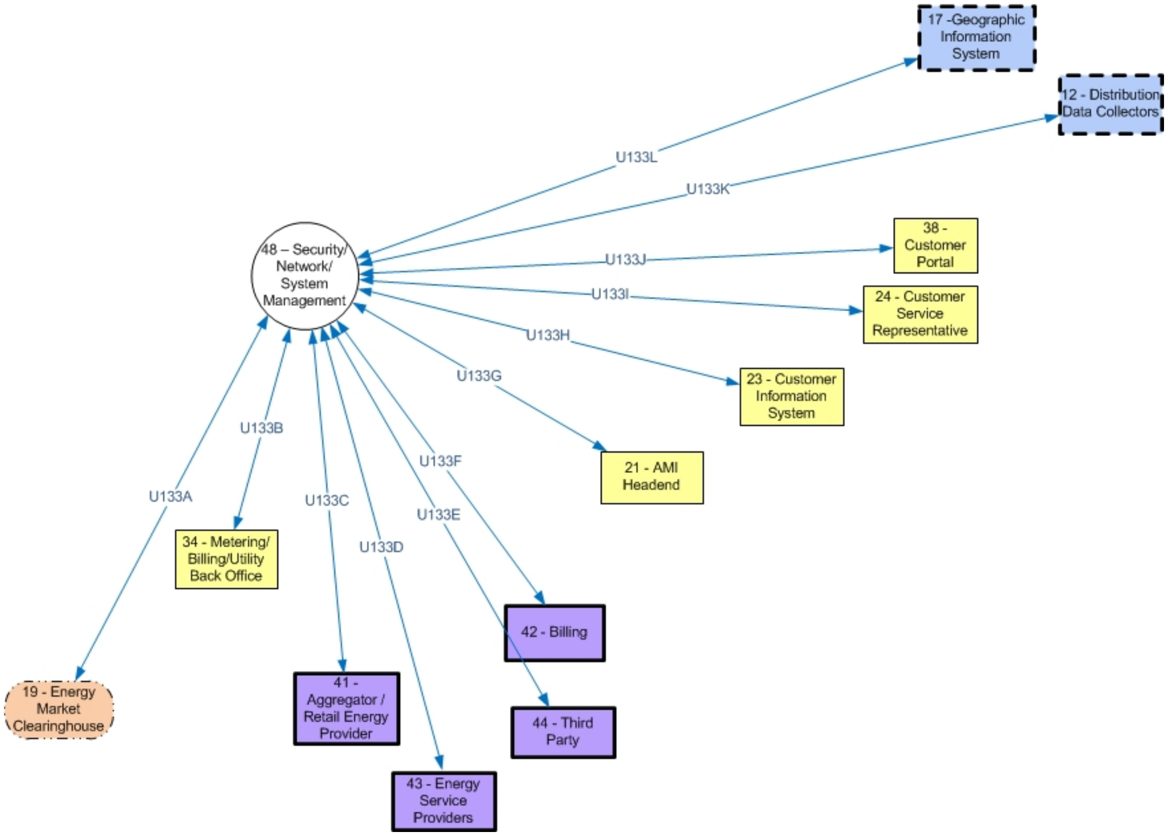

17 -Geographic Information System
12 - Distribution Data Collectors
U133L
U133K
38 - Customer Portal
U133J
48 – Security/ Network/ System Management
U133I
24 - Customer Service Representative
U133H
23 - Customer Information System
U133G
21 - AMI Headend
U133B
U133A
U133F
U133C
U133E
34 - Metering/ Billing/Utility Back Office
U133D
42 - Billing
19 - Energy Market Clearinghouse
41 - Aggregator / Retail Energy Provider
44 - Third Party
43 - Energy Service Providers

Figure 3-19
Logical Interface Category 22: Interface Between Security/Network/System Management Consoles and All Networks and Systems

[The diagram was extracted from the NISTIR 7628]

Unique Technical Requirements:

- SG.AC-12: Session Lock
  - There are no associated ES-C2M2 practices.
- SG.AC-14: Permitted Actions without Identification and Authentication
  - The associated ES-C2M2 practice is IAM-2a.
- SG.AC-15: Remote Access
  - The associated ES-C2M2 practices are: IAM-2a, IAM-2b, IAM-2c, IAM-2e, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, and SA-2i
- SG.AU-16: Non-Repudiation
  - There are no associated ES-C2M2 practices.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b.
- SG.IA-6: Authenticator Feedback
  - The associated ES-C2M2 practice is IAM-3e.
- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is CPM-3b.
- SG.SC-5: Denial-of-Service Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, and CPM-3b.
- SG.SC-6: Resource Priority
  - The associated ES-C2M2 practices are ACM-1b, ACM-1c, and ACM-1d.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are TVM-1c, TVM-2c, SA-2a, SA-2b, SA-2e, SA-2f, SA-2g, SA-2j, CPM-3a, CPM-3b, CPM-3c, and CPM-3d.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SC-9: Communication Confidentiality
  - The associated ES-C2M2 practices are TVM-1c and TVM-2c.
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i.

3.1 Tailored ES-C2M2 Practices

Listed below are the NISTIR 7628 security requirements, the associated ES-C2M2 practices, and a description related to each practice that is tailored to the security requirement. The security requirements are listed in alphabetical order.

- SG.AC-12:
  - There are no associated ES-C2M2 practices.
- SG.AC-13:
  - The associated ES-C2M2 practice is:
    - IAM-2a: remote session access is terminated at the end of the session or after an organization-defined period.
- SG.AC-14: Permitted Actions without Identification or Authentication
  - The associated ES-C2M2 practice is:
    - IAM-2a: access requirements are determined, including the type of access.
- SG.AC-15:
  - The associated ES-C2M2 practices:
    - IAM-2a: remote access requirements are specified and implemented.
    - IAM-2b: remote access is granted based on requirements.
    - IAM-2c: remote access is revoked when it is no longer needed.
    - IAM-2e: remote access to control systems is granted after approval by the asset owner.
    - SA-2a: remote access to the system is monitored, including monitoring for unauthorized remote access.
    - SA-2b: remote access to the system is monitored for anomalous behavior that may indicate a cyber security event.
    - SA-2e: remote access is monitored for identified anomalous activity.
    - SA-2f: remote access monitoring is based on threat information.
    - SA-2g: remote access monitoring is based on the risk to the function.
    - SA-2i: continuous remote access monitoring is performed across the operational environment
- SG.AU-16:
  - There are no associated ES-C2M2 practices.
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are:
    - IAM-1a: identities are provisioned for individuals.
    - IAM-1b: credentials are provisioned for individuals.
- SG.IA-5: Device Identification and Authentication
  - The associated ES-C2M2 practices are:
    - IAM-1a: credentials are provisioned for individuals.
    - IAM-1b: credentials are provisioned for devices.
- SG.IA-6: Authenticator Feedback:
  - The associated ES-C2M2 practice is:
    - IAM-3e: access management activities are guided by documented organization policies/directives.

- SG.SC-3: Security Function Isolation
  - The associated ES-C2M2 practice is
    - CPM-3b: a cyber security architecture is specified and implemented to isolate security functions (hardware, software, and/or firmware) from non-security functions.
- SG.SC-5: Denial-of-Service Protection:
  - The associated ES-C2M2 practices are:
    - TVM-1c: the system implements mitigations for denial-of-service attacks based on threat information.
    - TVM-2c: the system implements mitigations for denial-of-service attacks based on vulnerability information.
    - CPM-3b: a cyber security architecture is specified and implemented to address denial-of-service security requirements.
- SG.SC-7: Boundary Protection
  - The associated ES-C2M2 practices are:
    - TVM-1c: the system implements boundary protection mitigations to protect communications at the external boundary and at key internal boundaries based on threat information.
    - TVM-2c: the system implements boundary protection mitigations to protect communications at the external boundary and at key internal boundaries based on vulnerability information.
    - SA-2a: cyber security monitoring is implemented at the boundary, specifically at managed interfaces.
    - SA-2b: cyber security monitoring is implemented at the boundary to identify anomalous behavior that may indicate a cyber security event.
    - SA-2e: cyber security monitoring implemented at the boundary is configured to detect identified anomalous activity.
    - SA-2f: the cyber security monitoring implemented at the boundary is configured based on the threat profile.
    - SA-2g: the cyber security monitoring implemented at the boundary is configured based on risk.
    - SA-2j: the risk register content is used to configure the cyber security monitoring that is implemented at the boundary.
    - CPM-3a: boundary protection includes architecturally isolating the IT and OT systems.
    - CPM-3b: the cyber security architecture includes boundary protection to enable isolation, segmentation and other cyber security requirements.
    - CPM-3c: a documented plan is used in the development of the cyber security architecture that includes boundary protection.
    - CPM-3d: the cyber security architecture, including boundary protection, is updated at a regular interval.
- SG.SC-8: Communication Integrity
  - The associated ES-C2M2 practices are:

        - TVM-1c: the system implements communication integrity mechanisms based on threat information.
        - TVM-2c: the system implements communication integrity mechanisms based on vulnerability information.

- SG.SC-9:
    - The associated ES-C2M2 practices are:
        - TVM-1c: the system implements communication integrity mechanisms based on threat information.
        - TVM-2c: the system implements communication integrity mechanisms based on vulnerability information.
- SG.SC-26:
    - The associated ES-C2M2 practices are:
        - TVM-1c: the system implements communication integrity mechanisms based on threat information.
        - TVM-2c: the system implements communication integrity mechanisms based on vulnerability information.
- SG.SI-7: Software and Information Integrity
    - The associated ES-C2M2 practices are:
        - SA-2e: the system implements software and information integrity mechanisms to identify potential anomalous activities such as tampering, errors, and/or omissions.
        - SA-2i: software and information integrity mechanisms are implemented across the operational environment to identify anomalous activity.

4

GAP ANALYSIS

There are several NISTIR 7628 security requirements that are applicable at the system level, and currently are not allocated to either the NIST CSF or the ES-C2M2. These security requirements should be considered in future revisions to the ES-C2M2 as they are important for applying that document to systems. These include:

- SG.AU-8: Time Stamps
- SG.SC-11: Cryptographic Key Establishment and Management
- SG.SC-12: Use of Validated Cryptography
- SG.SC-15: Public Key Infrastructure Certificates
- SG.SC-22: Fail in Known State
- SG.SI-6: Security Functionality Verification
- SG.SI-8: Information Input Validation
- SG.SI-9: Error Handling

5
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 regulations, guidelines, and specifications. The application guidance included in this technical update, and the information included in the companion EPRI technical updates 3002004712, *Cyber Security Risk Management in Practice - Comparative Analyses Tables* and 3002003333, *Risk Management in Practice - A Guide for the Electric Sector* are intended to provide this 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 baseline 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. Also under consideration is adding additional international standards and guidelines to the tables, for example, ISO standards.

6
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. U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Risk Management Process*, May 2012 [government publication].
5. U.S. Department of Energy (DOE), *Energy Sector Cybersecurity Framework Implementation Guidance*, draft for public comment, September 2014 [government publication].
6. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014 [government publication].
7. Office of the President, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, February 12, 2013 [government publication].
8. EPRI and DOE, *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology*, EPRI technical update 3002001181, 2013 [report] (The document is posted as a joint DOE/EPRI publication at: http://energy.gov/sites/prod/files/2014/05/f15/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology_1.pdf)
9. 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].
10. Nuclear Regulatory Commission, Regulatory Guidance 5.71, *Cyber Security Programs for Nuclear Facilities*, January 2010 [government publication].
11. Nuclear Energy Institute, NEI 08-09 Revision 6, *Cyber Security Plan for Nuclear Power Reactors*, April 2010 [government publication].
12. SGIP CSWG – Test & Certification Subgroup, *Guide for Assessing the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cyber Security*, SGIP Document Number: 2012-004_1, Version 1.0, August 24, 2012 [report].

7
ACRONYMS

BES	Bulk Electric System
CIP	Critical Infrastructure Protection
COP	Common Operating Picture
CSF	Cybersecurity Framework
CSWG	Cyber Security Working Group
CTR	Common Technical Requirement
DHS	Department of Homeland Security
DOE	Department of Energy
EO	Executive Order
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
GRC	Governance, Risk, and Compliance
ICS	Industrial Control Systems
IT	Information Technology
MIL	Maturity Indicator Level
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NRECA	National Rural Electric Cooperative Association
OT	Operations Technology
PUC	Public Utility Commission
RMP	Risk Management Process
SGIP	Smart Grid Interoperability Panel
UTR	Unique Technical Requirement

A

ES-C2M2 AND NISTIR 7628 SECURITY REQUIREMENTS

Table A-1 below includes the allocation of the NISTIR 7628 security requirements to the individual ES-C2M2 practices. In addition, the table includes the assessment methods that may be used for each NISTIR 7628 security requirement. These methods are defined in the SGIP document *Guide for Assessing the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cyber Security* and are included here for completeness.

The assessment methods consist of examine, interview, and test, and define the nature of the assessor actions. An Assessor may use any or all of the assessment methods listed below:

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

In all three assessment methods, the results are used to make specific determinations.

Table A-1
ES-C2M2 and NISTIR 7628 Security Requirements

[The information in the following table was extracted from the ES-C2M2 and the NISTIR 7628.]

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
1. Establish Cyber Security Risk Management Strategy				
MIL1	No practice at MIL 1			
MIL2	a. There is a documented cybersecurity risk management strategy	SG.PM-5	GRC	Examine, Interview
	b. The strategy provides an approach for risk prioritization, including consideration of impact	SG.PM-5 SG.PM-7	GRC GRC	Examine, Interview Examine, Interview
MIL3	c. Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available	SG.CA-2 SG.CA-6 SG.PM-2 SG.PM-5 SG.PM-7 SG.RA-2 SG.RA-3 SG.RA-4 SG.RA-6 SG.SA-10 SG.SI-2	GRC GRC GRC GRC GRC GRC GRC GRC GRC GRC CTR	Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview, Test
	d. The risk management strategy is periodically updated to reflect the current threat environment	SG.PM-5	GRC	Examine, Interview
	e. An organization-specific risk taxonomy is documented and is used in risk management activities	SG.PM-5 SG.RA-2	GRC GRC	Examine, Interview Examine, Interview
2. Manage Cyber Security Risk				
MIL1	a. Cybersecurity risks are identified	SG.PzM-5	Z	Examine, Interview
	b. Identified risks are mitigated, accepted, tolerated, or transferred	SG.PM-5	GRC	Examine, Interview
MIL2	c. Risk assessments are performed to identify risks in accordance with the risk management strategy	SG.PM-5	GRC	Examine, Interview
	d. Identified risks are documented	SG.PM-5	GRC	Examine, Interview
	e. Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy	SG.PM-5	GRC	Examine, Interview
	f. Identified risks are monitored in accordance with the risk management strategy	There are no applicable NISTIR 7628 security requirements.		
	g. Risk analysis is informed by network (IT and/or OT) architecture	SG.PM-5	GRC	Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL3	h. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy	SG.PM-5	GRC	Examine, Interview
	i. A current cybersecurity architecture is used to inform risk analysis	SG.PM-5	GRC	Examine, Interview
	j. A risk register (a structured repository of identified risks) is used to support risk management activities	SG.PM-5	GRC	Examine, Interview
3. Management Activities				
MIL1	No practice at MIL 1			
MIL2	a. Documented practices are followed for risk management activities	SG.PM-5	GRC	Examine, Interview
	b. Stakeholders for risk management activities are identified and involved	SG.PM-5	GRC	Examine, Interview
	c. Adequate resources (people, funding, and tools) are provided to support risk management activities	SG.PM-5	GRC	Examine, Interview
	d. Standards and/or guidelines have been identified to inform risk management activities	SG.PM-5	GRC	Examine, Interview
MIL3	e. Risk management activities are guided by documented policies or other organizational directives	SG.RA-1	GRC	Examine, Interview
	f. Risk management policies include compliance requirements for specified standards and/or guidelines	SG.RA-1 SG.PE-1	GRC GRC	Examine, Interview Examine, Interview
	g. Risk management activities are periodically reviewed to ensure conformance with policy	SG.PM-5	GRC	Examine, Interview
	h. Responsibility and authority for the performance of risk management activities are assigned to personnel	SG.PM-5	GRC	Examine, Interview
	i. Personnel performing risk management activities have the skills and knowledge needed to perform their assigned responsibilities	SG.PM-5	GRC	Examine, Interview
Asset, Change and Configuration Management				
1. Manage Asset Inventory				
MIL1	a. There is an inventory of OT and IT assets that are important to the delivery of the function	SG.CM-2 SG.CM-8	GRC GRC	Examine, Interview Examine, Interview
	b. There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data)	SG.CP-9 SG.RA-3 SG.SC-6	GRC GRC UTR	Examine Examine, Interview Examine, Test
MIL2	c. Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)	SG.CM-8 SG.RA-3 SG.SC-6	GRC GRC UTR	Examine, Interview Examine, Interview Examine, Test
	d. Inventoried assets are prioritized based on their importance to the delivery of the function	SG.CP-2 SG.CP-9 SG.SC-6	GRC GRC UTR	Examine, Interview Examine Examine, Test

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL3	e. There is an inventory for all connected IT and OT assets related to the delivery of the function	SG.CA-4 SG.CM-8 SG.PM-4 SG.SA-11	GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine Examine
	f. The asset inventory is current (as defined by the organization)	SG.CM-8	GRC	Examine, Interview
2. Manage Asset Configuration				
MIL1	a. Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly	SG.CM-2 SG.CM-6 SG.SA-9	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
	b. Configuration baselines are used to configure assets at deployment	SG.CM-2 SG.CM-6 SG.SA-9	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
MIL2	c. The design of configuration baselines includes cybersecurity objectives	SG.CM-7	CTR	Examine, Interview, Test
MIL3	d. Configuration of assets are monitored for consistency with baselines throughout the assets' life cycle	SG.CM-2	GRC	Examine, Interview
	e. Configuration baselines are reviewed and updated at an organizationally-defined frequency	SG.CM-2	GRC	Examine, Interview
3. Manage Changes to Assets				
MIL1	a. Changes to inventoried assets are evaluated before being implemented	SG.CM-3 SG.CM-4 SG.MA-3	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
	b. Changes to inventoried assets are logged	SG.CM-6 SG.CM-8 SG.CM-9 SG.MA-3 SG.PE-10 SG.SA-9	GRC GRC GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview
MIL2	c. Changes to assets are tested prior to being deployed, whenever possible	SG.CM-2 SG.CM-3	GRC GRC	Examine, Interview Examine, Interview
	d. Change management practices address the full life cycle of assets (i.e., acquisition, deployment, operation, retirement)	SG.CM-3 SG.CM-9 SG.CM-10 SG.MP-6 SG.PE-10 SG.SA-3 SG.SA-8 SG.SA-9 SG.SA-10	GRC GRC GRC GRC GRC GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL3	e. Changes to assets are tested for cybersecurity impact prior to being deployed	SG.CM-2 SG.CM-4	GRC GRC	Examine, Interview Examine, Interview
	f. Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)	SG.MA-3	GRC	Examine, Interview
4. Management Activities				
MIL1	No practice at MIL 1			
MIL2	a. Documented practices are followed for asset inventory, configuration, and change management activities	SG.CM-3 SG.CM-4 SG.CM-5 SG.CM-6 SG.CM-8 SG.CM-9 SG.CM-10 SG.CM-11 SG.MP-6 SG.PE-10 SG.SA-9	GRC GRC GRC GRC GRC GRC GRC GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview
	b. Stakeholders for asset inventory, configuration, and change management activities are identified and involved	SG.CM-8	GRC	Examine, Interview
	c. Adequate resources (people, funding, and tools) are provided to support asset inventory, configuration, and change management activities	SG.MA-4 SG.MA-5 SG.MA-7	GRC GRC GRC	Examine Examine, Interview Examine, Interview
	d. Standards and/or guidelines have been identified to inform asset inventory, configuration, and change management activities	SG.CM-8 SG.MP-6	GRC GRC	Examine, Interview Examine, Interview
MIL3	e. Asset inventory, configuration, and change management activities are guided by documented policies or other organizational directives	SG.CM-3 SG.CM-4 SG.CM-6 SG.CM-8 SG.CM-9	GRC GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview
	f. Asset inventory, configuration, and change management policies include compliance requirements for specified standards and/or guidelines	SG.PE-1 SG.PE-12	GRC GRC	Examine, Interview Examine, Interview
	g. Asset inventory, configuration, and change management activities are periodically reviewed to ensure conformance with policy	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	h. Responsibility and authority for the performance of asset inventory, configuration, and change management activities are assigned to personnel	There are no applicable NISTIR 7628 security requirements.		
	i. Personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities	There are no applicable NISTIR 7628 security requirements.		
Identity and Access Management				
1. Establish and Maintain Identities				
MIL1	a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)	SG.AC-3 SG.IA-2 SG.IA-4 SG.IA-5	GRC GRC UTR UTR	Examine, Interview Examine, Interview Examine, Test Examine, Test
	b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)	SG.AC-19 SG.AC-21 SG.IA-3 SG.IA-4 SG.IA-5	CTR GRC GRC UTR UTR	Examine, Interview, Test Examine, Test Examine, Interview, Test Examine, Test Examine, Test
	c. Identities are deprovisioned when no longer required	SG.AC-3	GRC	Examine, Interview
MIL2	d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access)	SG.AC-3	GRC	Examine, Interview
	e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity	SG.AC-3 SG.IA-3	GRC GRC	Examine, Interview Examine, Interview, Test
	f. Identities are deprovisioned within organizationally defined time thresholds when no longer required	SG.AC-3	GRC	Examine, Interview
MIL3	g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RM-1c)	SG.IA-4	UTR	
2. Control Access				

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL1	a. Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)	SG.AC-2 SG.AC-4 SG.AC-13 SG.AC-14 SG.AC-15 SG.AC-17 SG.MA-6 SG.MP-4 SG.MP-5 SG.PE-2	GRC GRC UTR UTR UTR GRC GRC GRC GRC GRC	Examine, Interview, Test Examine Examine, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview Examine, Interview
	b. Access is granted to identities based on requirements	SG.AC-2 SG.AC-4 SG.AC-15 SG.AC-17 SG.MA-6 SG.MP-4 SG.MP-5 SG.PE-3	GRC GRC UTR GRC GRC GRC GRC GRC	Examine, Interview, Test Examine Examine, Interview, Test Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview Examine, Interview, Test
	c. Access is revoked when no longer required	SG.AC-15 SG.MA-6 SG.PE-2 SG.SA-2	UTR GRC GRC GRC	Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview
MIL2	d. Access requirements incorporate least privilege and separation of duties principles	SG.AC-6 SG.AC-7	GRC GRC	Examine, Interview, Test Examine, Interview, Test
	e. Access requests are reviewed and approved by the asset owner	SG.AC-15 SG.MA-6 SG.PE-2	UTR GRC GRC	Examine, Interview, Test Examine, Interview Examine, Interview
	f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring	SG.AC-3 SG.PE-2	UTR GRC	Examine, Interview, Test Examine, Interview
MIL3	g. Access privileges are reviewed and updated to ensure validity, at an organizationally defined frequency	SG.PE-2	GRC	Examine, Interview Examine, Interview
	h. Access to assets is granted by the asset owner based on risk to the function	SG.MA-6	GRC	Examine, Interview
	i. Anomalous access attempts are monitored as indicators of cybersecurity events	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
3. Management Activities				
MIL1	No practice at MIL 1			
MIL2	a. Documented practices are followed to establish and maintain identities and control access	SG.AC-8 SG.AC-10 SG.AC-12 SG.IA-6	CTR UTR UTR UTR	Examine, Test Examine, Test Examine, Test Examine, Test
	b. Stakeholders for access and identity management activities are identified and involved	There are no applicable NISTIR 7628 security requirements.		
	c. Adequate resources (people, funding, and tools) are provided to support access and identity management activities	There are no applicable NISTIR 7628 security requirements.		
	d. Standards and/or guidelines have been identified to inform access and identity management activities	There are no applicable NISTIR 7628 security requirements.		
MIL3	e. Access and identity management activities are guided by documented policies or other organizational directives	SG.AC-1 SG.IA-1	GRC GRC	Examine, Interview Examine, Interview
	f. Access and identity management policies include compliance requirements for specified standards and/or guidelines	SG.IA-1	GRC	Examine, Interview
	g. Access and identity management activities are periodically reviewed to ensure conformance with policy	There are no applicable NISTIR 7628 security requirements.		
	h. Responsibility and authority for the performance of access and identity management activities are assigned to personnel	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	i. Personnel performing access and identity management activities have the skills and knowledge needed to perform their assigned responsibilities	There are no applicable NISTIR 7628 security requirements.		
Threat and Vulnerability Management				
1. Identify and Respond to Threats				
MIL1	a. Information sources to support threat management activities are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associates, vendors, federal briefings)	SG.AT-5 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview
	b. Cybersecurity threat information is gathered and interpreted for the function	SG.AT-5 SG.RA-4 SG.SI-5	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
	c. Threats that are considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status)	SG.AC-6 SG.AC-7 SG.SC-5 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-12 SG.SC-26	GRC GRC UTR UTR UTR UTR CTR UTR	Examine, Interview, Test Examine, Interview, Test Examine, Test Examine, Interview, Test Examine, Test Examine, Test Examine Examine, Test
MIL2	d. A threat profile for the function is established that includes characterization of likely intent, capability, and target of threats to the function	SG.RA-3 SG.RA-4	GRC GRC	Examine, Interview Examine, Interview
	e. Threat information sources that address all components of the threat profile are prioritized and monitored	SG.RA-4 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview
	f. Identified threats are analyzed and prioritized	SG.PM-5	GRC	Examine, Interview
	g. Threats are addressed according to the assigned priority	There are no applicable NISTIR 7628 security requirements.		
MIL3	h. The threat profile for the function is validated at an organization-defined frequency	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	i. Analysis and prioritization of threats are informed by the function's (or organization's) risk criteria (RM-1c)	There are no applicable NISTIR 7628 security requirements.		
	j. Threat information is added to the risk register (RM-2j)	There are no applicable NISTIR 7628 security requirements.		Examine, Interview
2. Reduce Cybersecurity Vulnerabilities				
MIL1	a. Information sources to support cybersecurity vulnerability discovery are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments)	SG.AT-5 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview
	b. Cybersecurity vulnerability information is gathered and interpreted for the function	SG.AT-5 SG.CA-2 SG.CA-6 SG.RA-6 SG.SA-10 SG.SI-2 SG.SI-5	GRC GRC GRC GRC GRC CTR GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview, Test Examine, Interview
	c. Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches)	SG.AC-6 SG.AC-7 SG.RA-6 SG.SC-5 SG.SC-7 SG.SC-8 SG.SC-9 SG.SC-12 SG.SC-26	GRC GRC GRC UTR UTR UTR UTR CTR UTR	Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Test Examine, Interview, Test Examine, Test Examine, Test Examine Examine, Test
MIL2	d. Cybersecurity vulnerability information sources that address all assets important to the function are monitored	SG.AT-5 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview
	e. Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools)	SG.CA-2 SG.CA-6 SG.RA-6 SG.SA-10	GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	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)	There are no applicable NISTIR 7628 security requirements.		
	g. Cybersecurity vulnerabilities are addressed according to the assigned priority	SG.RA-6	GRC	Examine, Interview, Test
	h. Operational impact to the function is evaluated prior to deploying cybersecurity patches	There are no applicable NISTIR 7628 security requirements.		
MIL3	i. Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function, at an organization-defined frequency	SG.CA-2 SG.CA-6 SG.RA-6 SG.SA-10 SG.SI-2	GRC GRC GRC GRC CTR	Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview, Test
	j. Cybersecurity vulnerability assessments are informed by the function’s (or organization’s) risk criteria (RM-1c)	SG.CA-2 SG.CA-6 SG.RA-6 SG.SA-10 SG.SI-2	GRC GRC GRC GRC CTR	Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview, Test
	k. Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function	SG.CA-2 SG.CA-6 SG.RA-6 SG.SA-10 SG.SI-2	GRC GRC GRC GRC CTR	Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview, Test
	l. Analysis and prioritization of cybersecurity vulnerabilities are informed by the function’s (or organization’s) risk criteria (RM-1c)	There are no applicable NISTIR 7628 security requirements.		
	m. Cybersecurity vulnerability information is added to the risk register (RM-2j)	SG.RA-6	GRC	Examine, Interview, Test
	n. Risk monitoring activities validate the responses to cybersecurity vulnerabilities (e.g., deployment of patches or other activities)	SG.RA-6	GRC	Examine, Interview, Test
3. Management Activities				
MIL1	No practice at MIL 1			

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL2	a. Documented practices are followed for threat and vulnerability management activities	SG.RA-4 SG.RA-5 SG.RA-6 SG.SI-2	GRC GRC GRC CTR	Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview, Test
	b. Stakeholders for threat and vulnerability management activities are identified and involved	There are no applicable NISTIR 7628 security requirements.		
	c. Adequate resources (people, funding, and tools) are provided to support threat and vulnerability management activities	There are no applicable NISTIR 7628 security requirements.		
	d. Standards and/or guidelines have been identified to inform threat and vulnerability management activities	There are no applicable NISTIR 7628 security requirements.		
MIL3	e. Threat and vulnerability activities are guided by documented policies or other organizational directives	There are no applicable NISTIR 7628 security requirements.		
	f. Threat and vulnerability management policies include compliance requirements for specified standards and/or guidelines	SG.RA-1	GRC	Examine, Interview
	g. Threat and vulnerability management activities are periodically reviewed to ensure conformance with policy	There are no applicable NISTIR 7628 security requirements.		
	h. Responsibility and authority for the performance of threat and vulnerability management activities are assigned to personnel	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	i. Personnel performing threat and vulnerability management activities have the skills and knowledge needed to perform their assigned responsibilities	There are no applicable NISTIR 7628 security requirements.		
Situational Awareness				
1. Perform Logging				
MIL1	a. Logging is occurring for assets important to the function where possible	SG.AU-2	GRC	Examine, Test
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])	SG.AU-2 SG.AU-15	GRC CTR	Examine, Test Examine, Interview
	c. Log data are being aggregated within the function	SG.AU-6	GRC	Examine, Interview, Test
MIL3	d. Logging requirements are based on the risk to the function	SG.AU-6 SG.AU-15	GRC CTR	Examine, Interview, Test Examine, Interview
	e. Log data support other business and security processes (e.g., incident response, asset management)	SG.AU-6	GRC	Examine, Interview, Test
2. Perform Monitoring				
MIL1	a. Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)	SG.AC-15 SG.AC-16 SG.AC-17 SG.AU-6 SG.CA-6 SG.CM-4 SG.PE-4 SG.PS-1 SG.PS-7 SG.SC-7 SG.SC-16 SG.SI-3 SG.SI-4	UTR GRC GRC GRC GRC GRC GRC GRC GRC UTR CTR CTR CTR	Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	b. Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event	SG.AC-15	UTR	Examine, Interview, Test
		SG.AC-16	GRC	Examine, Interview, Test
		SG.AC-17	GRC	Examine, Interview, Test
		SG.CM-4	GRC	Examine, Interview
		SG.PE-4	GRC	Examine, Interview, Test
		SG.SC-7	UTR	Examine, Interview, Test
		SG.SC-16	CTR	Examine, Interview, Test
		SG.SI-3	CTR	Examine, Interview, Test
		SG.SI-4	CTR	Examine, Interview, Test
MIL2	c. Monitoring and analysis requirements have been defined for the function and address timely review of event data	SG.AU-6	GRC	Examine, Interview, Test
		SG.AU-15	CTR	Examine, Interview
	d. Alarms and alerts are configured to aid in the identification of cybersecurity events (IR-1b)	SG.SI-4	CTR	Examine, Interview, Test
	e. Indicators of anomalous activity have been defined and are monitored across the operational environment	SG.AC-15	UTR	Examine, Interview, Test
		SG.AC-16	GRC	Examine, Interview, Test
		SG.AC-17	GRC	Examine, Interview, Test
		SG.CM-4	GRC	Examine, Interview
		SG.PE-4	GRC	Examine, Interview, Test
		SG.PS-1	GRC	Examine, Interview
		SG.PS-7	GRC	Examine, Interview
		SG.SC-7	UTR	Examine, Interview, Test
		SG.SC-16	CTR	Examine, Interview, Test
		SG.SI-3	CTR	Examine, Interview, Test
		SG.SI-4	CTR	Examine, Interview, Test
		SG.SI-7	UTR	Examine, Interview, Test
	f. Monitoring activities are aligned with the function’s threat profile (TVM-1d)	SG.AC-15	UTR	Examine, Interview, Test
		SG.AC-17	GRC	Examine, Interview, Test
		SG.SC-7	UTR	Examine, Interview, Test
		SG.SI-4	CTR	Examine, Interview, Test
MIL3	g. Monitoring requirements are based on the risk to the function	SG.AC-15	UTR	Examine, Interview, Test
		SG.AC-16	GRC	Examine, Interview, Test
		SG.AC-17	GRC	Examine, Interview, Test
		SG.CA-6	GRC	Examine, Interview
		SG.SC-7	UTR	Examine, Interview, Test
		SG.SI-4	CTR	Examine, Interview, Test
	h. Monitoring is integrated with other business and security processes (e.g., incident response, asset management)	SG.SC-16	CTR	Examine, Interview, Test

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	i. Continuous monitoring is performed across the operational environment to identify anomalous activity	SG.AC-15 SG.AC-16 SG.AC-17 SG.CM-4 SG.PE-4 SG.SC-7 SG.SC-16 SG.SI-3 SG.SI-4 SG.SI-7	UTR GRC GRC GRC GRC UTR CTR CTR CTR UTR	Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test Examine, Interview, Test
	j. Risk register (RM-2j) content is used to identify indicators of anomalous activity	There are no applicable NISTIR 7628 security requirements.		
	k. Alarms and alerts are configured according to indicators of anomalous activity	There are no applicable NISTIR 7628 security requirements.		
3. Establish and Maintain a Common Operating Picture (COP)				
MIL1	No practice at MIL 1			
MIL2	a. Methods of communicating the current state of cybersecurity for the function are established and maintained	There are no applicable NISTIR 7628 security requirements.		
	b. Monitoring data are aggregated to provide an understanding of the operational state of the function (i.e., a common operating picture; a COP may or may not include visualization or be presented graphically)	There are no applicable NISTIR 7628 security requirements.		
	c. Information from across the organization is available to enhance the common operating picture	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL3	d. Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for the function to enhance the common operating picture	SG.AU-7	CTR	Examine, Interview, Test
	e. Information from outside the organization is collected to enhance the common operating picture	There are no applicable NISTIR 7628 security requirements.		
	f. Predefined states of operation are defined and invoked (manual or automated process) based on the common operating picture	There are no applicable NISTIR 7628 security requirements.		
4. Management Activities				
MIL1	No practice at MIL 1			
MIL2	a. Documented practices are followed for logging, monitoring, and COP activities	SG.AU-3 SG.AU-4 SG.AU-5 SG.AU-9 SG.AU-10 SG.AU-11 SG.AU-13 SG.PE-5 SG.PE-6 SG.PE-7	CTR GRC CTR CTR GRC GRC GRC GRC GRC GRC	Examine, Test Examine, Test Examine, Test Examine, Test Examine, Interview Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview
	b. Stakeholders for logging, monitoring, and COP activities are identified and involved	There are no applicable NISTIR 7628 security requirements.		
	c. Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	d. Standards and/or guidelines have been identified to inform logging, monitoring, and COP activities	There are no applicable NISTIR 7628 security requirements.		
MIL3	e. Logging, monitoring, and COP activities are guided by documented policies or other organizational directives	SG.AU-1	GRC	Examine, Interview
	f. Logging, monitoring, and COP policies include compliance requirements for specified standards and/or guidelines	SG.AU-1 SG.SC-1 SG.SI-1	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
	g. Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy	SG.AU-1	GRC	Examine, Interview
	h. Responsibility and authority for the performance of logging, monitoring, and COP activities are assigned to personnel	There are no applicable NISTIR 7628 security requirements.		
	i. Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities	There are no applicable NISTIR 7628 security requirements.		
Information Sharing and Communications				
1. Share Cybersecurity Information				
MIL1	a. Information is collected from and provided to selected individuals and/or organizations	SG.AT-5 SG.AU-6 SG.CP-2 SG.IR-7 SG.IR-11 SG.SI-5	GRC GRC GRC GRC GRC GRC	Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview Examine, Interview
	b. Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, DOE Form OE-417, ES-ISAC, ICS-CERT, law enforcement)	SG.AT-5 SG.CP-2 SG.IR-11	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
MIL2	c. Information-sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected utilities, vendors, sector organizations, regulators, internal entities)	SG.AT-5 SG.CP-2 SG.IR-11 SG.SI-5	GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview
	d. Information is collected from and provided to identified information-sharing stakeholders	SG.AT-5 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	e. Technical sources are identified that can be consulted on cybersecurity issues	SG.AT-5 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview
	f. Provisions are established and maintained to enable secure sharing of sensitive or classified information	SG.AT-5 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview
	g. Information-sharing practices address both standard operations and emergency operations	SG.AT-5	GRC	Examine, Interview
MIL3	h. Information-sharing stakeholders are identified based on shared interest in and risk to critical infrastructure	SG.AT-5 SG.AU-6 SG.SI-5	GRC GRC GRC	Examine, Interview Examine, Interview, Test Examine, Interview
	i. The function or the organization participates with information sharing and analysis centers	SG.AT-5 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview
	j. Information-sharing requirements have been defined for the function and address timely dissemination of cybersecurity information	SG.AT-5	GRC	Examine, Interview
	k. Procedures are in place to analyze and de-conflict received information	There are no applicable NISTIR 7628 security requirements.		
	l. A network of internal and external trust relationships (formal and/or informal) has been established to vet and validate information about cyber events	SG.AT-5 SG.SI-5	GRC GRC	Examine, Interview Examine, Interview
2. Management Activities				
MIL1	No practice at MIL 1			
MIL2	a. Documented practices are followed for information-sharing activities	There are no applicable NISTIR 7628 security requirements.		
	b. Stakeholders for information-sharing activities are identified and involved	There are no applicable NISTIR 7628 security requirements.		
	c. Adequate resources (people, funding, and tools) are provided to support information-sharing activities	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	d. Standards and/or guidelines have been identified to inform information-sharing activities	There are no applicable NISTIR 7628 security requirements.		
MIL3	e. Information-sharing activities are guided by documented policies or other organizational directives	There are no applicable NISTIR 7628 security requirements.		
	f. Information-sharing policies include compliance requirements for specified standards and/or guidelines	SG.ID-1 SG.MP-1	GRC GRC	Examine, Interview Examine, Interview
	g. Information-sharing activities are periodically reviewed to ensure conformance with policy	There are no applicable NISTIR 7628 security requirements.		
	h. Responsibility and authority for the performance of information-sharing activities are assigned to personnel	There are no applicable NISTIR 7628 security requirements.		
	i. Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities	There are no applicable NISTIR 7628 security requirements.		
	j. Information-sharing policies address protected information and ethical use and sharing of information, including sensitive and classified information as appropriate	There are no applicable NISTIR 7628 security requirements.		
Event and Incident Response, Continuity of Operations				
1. Detect Cybersecurity Events				
MIL1	a. There is a point of contact (person or role) to whom cybersecurity events could be reported	SG.IR-7	GRC	Examine, Interview
	b. Detected cybersecurity events are reported	SG.AU-6 SG.IR-7	GRC GRC	Examine, Interview, Test Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	c. Cybersecurity events are logged and tracked	There are no applicable NISTIR 7628 security requirements.		
MIL2	d. Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events)	SG.CP-2	GRC	Examine, Interview
	e. There is a repository where cybersecurity events are logged based on the established criteria	SG.IR-5 SG.IR-6	GRC GRC	Examine, Interview, Test Examine, Interview, Test
MIL3	f. Event information is correlated to support incident analysis by identifying patterns, trends, and other common features	SG.AU-6 SG.IR-5 SG.IR-8	GRC GRC GRC	Examine, Interview, Test Examine, Interview, Test Examine, Interview
	g. Cybersecurity event detection activities are adjusted based on information from the organization's risk register (RM-2j) and threat profile (TVM-1d) to help detect known threats and monitor for identified risks	There are no applicable NISTIR 7628 security requirements.		
	h. The common operating picture for the function is monitored to support the identification of cybersecurity events (SA-3a)	There are no applicable NISTIR 7628 security requirements.		
2. Escalate Cybersecurity Events and Declare Incidents				
MIL1	a. Criteria for cybersecurity event escalation are established, including cybersecurity incident declaration criteria	SG.SI-4	CTR	Examine, Interview, Test
	b. Cybersecurity events are analyzed to support escalation and the declaration of cybersecurity incidents	SG.IR-5	GRC	Examine, Interview, Test
	c. Escalated cybersecurity events and incidents are logged and tracked	There are no applicable NISTIR 7628 security requirements.		
MIL2	d. Criteria for cybersecurity event escalation, including cybersecurity incident criteria, are established based on the potential impact to the function	SG.IR-5 SG.SI-4	GRC CTR	Examine, Interview, Test Examine, Interview, Test

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	e. Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are updated at an organization-defined frequency	There are no applicable NISTIR 7628 security requirements.		
	f. There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure	There are no applicable NISTIR 7628 security requirements.		
MIL3	g. Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are adjusted according to information from the organization's risk register (RM-2j) and threat profile (TVM-1d)	SG.SI-4	CTR	Examine, Interview, Test
	h. Escalated cybersecurity events and declared cybersecurity incidents inform the common operating picture (SA-3a) for the function	There are no applicable NISTIR 7628 security requirements.		
	i. Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features	SG.AU-6 SG.IR-5	GRC GRC	Examine, Interview, Test Examine, Interview, Test
3. Respond to Incidents and Escalated Cybersecurity Events				
MIL1	a. Cybersecurity event and incident response personnel are identified and roles are assigned	SG.CP-3 SG.IR-2 SG.IR-11	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
	b. Responses to escalated cybersecurity events and incidents are implemented to limit impact to the function and restore normal operations	SG.CP-2 SG.IR-5	GRC GRC	Examine, Interview Examine, Interview, Test
	c. Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, DOE Form OE-417, ES-ISAC, ICS-CERT)	SG.AU-6 SG.IR-7	GRC GRC	Examine, Interview, Test Examine, Interview
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)	SG.CP-2 SG.CP-10 SG.IR-5	GRC GRC GRC	Examine, Interview Examine, Interview, Test Examine, Interview, Test
	e. Cybersecurity event and incident response plans are exercised at an organization- defined frequency	SG.IR-4 SG.SI-4	GRC CTR	Examine, Interview Examine, Interview, Test

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	f. Cybersecurity event and incident response plans address OT and IT assets important to the delivery of the function	SG.CP-2 SG.IR-1 SG.IR-2	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
	g. Training is conducted for cybersecurity event and incident response teams	There are no applicable NISTIR 7628 security requirements.		
MIL3	h. Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken	SG.CA-3 SG.CP-2 SG.IR-5 SG.IR-8 SG.IR-9 SG.RA-6	GRC GRC GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview Examine, Interview, Test
	i. Cybersecurity event and incident responses are coordinated with law enforcement and other government entities as appropriate, including support for evidence collection and preservation	SG.CP-2 SG.IR-11	GRC GRC	Examine, Interview Examine, Interview
	j. Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., table top, simulated incidents)	There are no applicable NISTIR 7628 security requirements.		
	k. Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency	SG.CP-6 SG.IR-1 SG.IR-2 SG.IR-5	GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview, Test
	l. Cybersecurity event and incident response activities are coordinated with relevant external entities	SG.CP-2 SG.IR-11	GRC GRC	Examine, Interview Examine, Interview
	m. Cybersecurity event and incident response plans are aligned with the function's risk criteria (RM-1c) and threat profile (TVM-1d)	There are no applicable NISTIR 7628 security requirements.		
	n. Policy and procedures for reporting cybersecurity event and incident information to designated authorities conform with applicable laws, regulations, and contractual agreements	SG.IR-1 SG.IR-7	GRC GRC	Examine, Interview Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	o. Restored assets are configured appropriately and inventory information is updated following execution of response plans	There are no applicable NISTIR 7628 security requirements.		
4. Plan for Continuity				
MIL1	a. The activities necessary to sustain minimum operations of the function are identified	SG.CP-2 SG.CP-5 SG.CP-10	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview, Test
	b. The sequence of activities necessary to return the function to normal operation is identified	SG.CP-2 SG.CP-5 SG.CP-10	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview, Test
	c. Continuity plans are developed to sustain and restore operation of the function	SG.CP-2 SG.CP-10	GRC GRC	Examine, Interview Examine, Interview, Test
MIL2	d. Business impact analyses inform the development of continuity plans	There are no applicable NISTIR 7628 security requirements.		
	e. Recovery time objectives (RTO) and recovery point objectives (RPO) for the function are incorporated into continuity plans	There are no applicable NISTIR 7628 security requirements.		
	f. Continuity plans are evaluated and exercised	SG.CP-5	GRC	Examine, Interview
MIL3	g. Business impact analyses are periodically reviewed and updated	There are no applicable NISTIR 7628 security requirements.		
	h. RTO and RPO are aligned with the function's risk criteria (RM-1c)	SG.CP-6	GRC	Examine, Interview
	i. The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly	There are no applicable NISTIR 7628 security requirements.		
	j. Continuity plans are periodically reviewed and updated	SG.CP-6	GRC	Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	k. Restored assets are configured appropriately and inventory information is updated following execution of continuity plans	There are no applicable NISTIR 7628 security requirements.		
5. Management Activities				
MIL1	No practice at MIL 1			
MIL2	a. Documented practices are followed for cybersecurity event and incident response as well as continuity of operations activities	SG.CP-2 SG.CP-11 SG.IR-1 SG.IR-2	GRC CTR GRC GRC	Examine, Interview Examine, Interview, Test Examine, Interview Examine, Interview
	b. Stakeholders for cybersecurity event and incident response as well as continuity of operations activities are identified and involved	SG.CP-2 SG.CP-3 SG.IR-2 SG.IR-11	GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview
	c. Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response as well as continuity of operations activities	SG.CP-2 SG.IR-1 SG.IR-2	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
	d. Standards and/or guidelines have been identified to inform cybersecurity event and incident response as well as continuity of operations activities	SG.IR-11	GRC	Examine, Interview
MIL3	e. Cybersecurity event and incident response as well as continuity of operations activities are guided by documented policies or other organizational directives	SG.IR-1	GRC	Examine, Interview
	f. Cybersecurity event and incident response as well as continuity of operations policies include compliance requirements for specified standards and/or guidelines	SG.CA-6 SG.IR-1 SG.IR-2	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
	g. Cybersecurity event and incident response as well as continuity of operations activities are periodically reviewed to ensure conformance with policy	SG.IR-1 SG.IR-2	GRC GRC	Examine, Interview Examine, Interview
	h. Responsibility and authority for the performance of cybersecurity event and incident response as well as continuity of operations activities are assigned to personnel	SG.CP-3 SG.IR-2	GRC GRC	Examine, Interview Examine, Interview
	i. Personnel performing cybersecurity event and incident response as well as continuity of operations activities have the skills and knowledge needed to perform their assigned responsibilities	SG.IR-2	GRC	Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
Supply Chain and External Dependencies Management				
1. Identify Dependencies				
MIL1	a. Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function depend, including operating partners)	SG.AC-11 SG.SA-11	GRC GRC	Examine, Interview Examine
	b. Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners)	There are no applicable NISTIR 7628 security requirements.		
MIL2	c. Supplier dependencies are identified according to established criteria	SG.SA-11	GRC	Examine
	d. Customer dependencies are identified according to established criteria	SG.SA-11	GRC	Examine
	e. Single-source and other essential dependencies are identified	There are no applicable NISTIR 7628 security requirements.		
	f. Dependencies are prioritized	There are no applicable NISTIR 7628 security requirements.		
MIL3	g. Dependency prioritization and identification are based on the function’s or organization's risk criteria (RM-1c)	There are no applicable NISTIR 7628 security requirements.		
2. Manage Dependency Risk				
MIL1	a. Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed	SG.PS-7	GRC	Examine, Interview
	b. Cybersecurity requirements are considered when establishing relationships with suppliers and other third parties	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL2	c. Identified cybersecurity dependency risks are entered into the risk register (RM-2j)	There are no applicable NISTIR 7628 security requirements.		
	d. Contracts and agreements with third parties incorporate sharing of cybersecurity threat information	There are no applicable NISTIR 7628 security requirements.		
	e. Cybersecurity requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate	There are no applicable NISTIR 7628 security requirements.		
	f. Agreements with suppliers and other external entities include cybersecurity requirements	SG.SA-4	GRC	Examine, Interview
	g. Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet cybersecurity requirements	There are no applicable NISTIR 7628 security requirements.		
	h. Agreements with suppliers require notification of cybersecurity incidents related to the delivery of the product or service	There are no applicable NISTIR 7628 security requirements.		
	i. Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements	There are no applicable NISTIR 7628 security requirements.		
MIL3	j. Cybersecurity risks due to external dependencies are managed according to the organization’s risk management criteria and process	SG.SI-4	CTR	Examine, Interview, Test
	k. Cybersecurity requirements are established for supplier dependencies based on the organization’s risk criteria (RM-1c)	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	l. Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products	There are no applicable NISTIR 7628 security requirements.		
	m. Acceptance testing of procured assets includes testing for cybersecurity requirements	There are no applicable NISTIR 7628 security requirements.		
	n. Information sources are monitored to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services)	SG.PS-7	GRC	Examine, Interview
3. Management Activities				
MIL1	No practice at MIL 1			
MIL2	a. Documented practices are followed for managing dependency risk	There are no applicable NISTIR 7628 security requirements.		
	b. Stakeholders for managing dependency risk are identified and involved	There are no applicable NISTIR 7628 security requirements.		
	c. Adequate resources (people, funding, and tools) are provided to support dependency risk management	There are no applicable NISTIR 7628 security requirements.		
MIL3	e. Dependency risk management activities are guided by documented policies or other organizational directives	There are no applicable NISTIR 7628 security requirements.		
	f. Dependency risk management policies include compliance requirements for specified standards and/or guidelines	SG.SA-1	GRC	Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	g. Dependency risk management activities are periodically reviewed to ensure conformance with policy	There are no applicable NISTIR 7628 security requirements.		
	h. Responsibility and authority for the performance of dependency risk management are assigned to personnel	There are no applicable NISTIR 7628 security requirements.		
	i. Personnel performing dependency risk management have the skills and knowledge needed to perform their assigned responsibilities	There are no applicable NISTIR 7628 security requirements.		
Workforce Management				
1. Assign Cybersecurity Responsibilities				
MIL1	a. Cybersecurity responsibilities for the function are identified	SG.AT-3	GRC	Examine, Interview
		SG.CP-3	GRC	Examine, Interview
		SG.CP-4	GRC	Examine, Interview
		SG.IR-3	GRC	Examine, Interview
		SG.PL-3	GRC	Examine
		SG.PM-8	GRC	Examine, Interview
		SG.PS-9	GRC	Examine, Interview
		SG.SC-19	GRC	Examine, Interview
	b. Cybersecurity responsibilities are assigned to specific people	SG.CP-3	GRC	Examine, Interview
		SG.PL-3	GRC	Examine
		SG.PS-9	GRC	Examine, Interview
		SG.SC-19	GRC	Examine, Interview
MIL2	c. Cybersecurity responsibilities are assigned to specific roles, including external service providers	SG.AT-3	GRC	Examine, Interview
		SG.CP-3	GRC	Examine, Interview
		SG.CP-4	GRC	Examine, Interview
		SG.IR-3	GRC	Examine, Interview
		SG.PL-3	GRC	Examine
		SG.PM-8	GRC	Examine, Interview
		SG.PS-9	GRC	Examine, Interview
		SG.SC-19	GRC	Examine, Interview

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	d. Cybersecurity responsibilities are documented (e.g., in position descriptions)	SG.AT-3 SG.PS-9 SG.SC-19	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
MIL3	e. Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate	There are no applicable NISTIR 7628 security requirements.		
	f. Cybersecurity responsibilities are included in job performance evaluation criteria	There are no applicable NISTIR 7628 security requirements.		
	g. Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage	There are no applicable NISTIR 7628 security requirements.		
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	SG.PS-3	GRC	Examine, Interview
	b. Personnel termination procedures address cybersecurity	SG.PS-4	GRC	Examine, Interview
MIL2	c. Personnel vetting is performed at an organization-defined frequency for positions that have access to the assets required for delivery of the function	SG.PS-3	GRC	Examine, Interview
	d. Personnel transfer procedures address cybersecurity	SG.PS-5	GRC	Examine, Interview
MIL3	e. Risk designations are assigned to all positions that have access to the assets required for delivery of the function	SG.PS-2	GRC	Examine, Interview
	f. Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation	SG.PS-2 SG.PS-3	GRC GRC	Examine, Interview Examine, Interview
	g. Succession planning is performed for personnel based on risk designation	SG.PS-1 SG.PS-2	GRC GRC	Examine, Interview Examine, Interview
	h. A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures	SG.PS-7 SG.PS-8 SG.PS-9	GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview
3. Develop Cybersecurity Workforce				

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL1	a. Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities	SG.AT-2 ST.AT-3 ST.AT-7	GRC GRC GRC	Examine, Interview
MIL2	b. Cybersecurity knowledge, skill, and ability gaps are identified	SG.AT-2 ST.AT-3 ST.AT-7	GRC GRC GRC	Examine, Interview
	c. Identified gaps are addressed through recruiting and/or training	SG.AT-2 ST.AT-3	GRC GRC	Examine, Interview
	d. Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function (e.g., new personnel training, personnel transfer training)	SG.AT-2 ST.AT-3	GRC GRC	Examine, Interview
MIL3	e. Cybersecurity workforce management objectives that support current and future operational needs are established and maintained	There are no applicable NISTIR 7628 security requirements.		
	f. Recruiting and retention are aligned to support cybersecurity workforce management objectives	SG.PS-1	GRC	Examine, Interview
	g. Training programs are aligned to support cybersecurity workforce management objectives	SG.AT-2 SG.AT-7	GRC GRC	Examine, Interview Examine, Interview
	h. The effectiveness of training programs is evaluated at an organization-defined frequency and improvements are made as appropriate	SG.AT-2	GRC	Examine, Interview
	i. Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities	There are no applicable NISTIR 7628 security requirements.		
4. Increase Cybersecurity Awareness				
MIL1	a. Cybersecurity awareness activities occur	SG.AT-2	GRC	Examine, Interview
MIL2	b. Objectives for cybersecurity awareness activities are established and maintained	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	c. Cybersecurity awareness content is based on the organization's threat profile (TVM-1d)	There are no applicable NISTIR 7628 security requirements.		
MIL3	d. Cybersecurity awareness activities are aligned with the predefined states of operation (SA-3f)	There are no applicable NISTIR 7628 security requirements.		
	e. The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency and improvements are made as appropriate	There are no applicable NISTIR 7628 security requirements.		
5. Management Activities				
MIL1	No practice at MIL 1			
MIL2	a. Documented practices are followed for cybersecurity workforce management activities	SG.AT-1 SG.AT-4	GRC GRC	Examine, Interview Examine, Interview
	b. Stakeholders for cybersecurity workforce management activities are identified and involved	SG.PS-9	GRC	Examine, Interview
	c. Adequate resources (people, funding, and tools) are provided to support cybersecurity workforce management activities	There are no applicable NISTIR 7628 security requirements.		
	d. Standards and/or guidelines have been identified to inform cybersecurity workforce management activities	There are no applicable NISTIR 7628 security requirements.		
MIL3	e. Cybersecurity workforce management activities are guided by documented policies or other organizational directives	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	f. Cybersecurity workforce management policies include compliance requirements for specified standards and/or guidelines	There are no applicable NISTIR 7628 security requirements.		
	g. Cybersecurity workforce management activities are periodically reviewed to ensure conformance with policy	There are no applicable NISTIR 7628 security requirements.		
	h. Responsibility and authority for the performance of cybersecurity workforce management activities are assigned to personnel	There are no applicable NISTIR 7628 security requirements.		
	i. Personnel performing cybersecurity workforce management activities have the skills and knowledge needed to perform their assigned responsibilities	There are no applicable NISTIR 7628 security requirements.		
Cybersecurity Program Management				
1. Establish Cybersecurity Program Strategy				
MIL1	a. The organization has a cybersecurity program strategy	There are no applicable NISTIR 7628 security requirements.		
MIL2	b. The cybersecurity program strategy defines objectives for the organization’s cybersecurity activities	There are no applicable NISTIR 7628 security requirements.		
	c. The cybersecurity program strategy and priorities are documented and aligned with the organization’s strategic objectives and risk to critical infrastructure	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	d. The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities	There are no applicable NISTIR 7628 security requirements.		
	e. The cybersecurity program strategy defines the structure and organization of the cybersecurity program	There are no applicable NISTIR 7628 security requirements.		
	f. The cybersecurity program strategy is approved by senior management	There are no applicable NISTIR 7628 security requirements.		
MIL3	g. The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVM-1d)	SG.CA-2 SG.CA-3 SG.CA-6 SG.PL-2	GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview
2. Sponsor Cybersecurity Program				
MIL1	a. Resources (people, tools, and funding) are provided to support the cybersecurity program	There are no applicable NISTIR 7628 security requirements.		
	b. Senior management provides sponsorship for the cybersecurity program	SG.PM-3	GRC	Examine, Interview
MIL2	c. The cybersecurity program is established according to the cybersecurity program strategy	There are no applicable NISTIR 7628 security requirements.		
	d. Adequate funding and other resources (i.e., people and tools) are provided to establish and operate a cybersecurity program aligned with the program strategy	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
	e. Senior management sponsorship for the cybersecurity program is visible and active (e.g., the importance and value of cybersecurity activities is regularly communicated by senior management)	There are no applicable NISTIR 7628 security requirements.		
	f. If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program	There are no applicable NISTIR 7628 security requirements.		
	g. The development and maintenance of cybersecurity policies is sponsored	SG.PM-1	GRC	Examine, Interview
	h. Responsibility for the cybersecurity program is assigned to a role with requisite authority	There are no applicable NISTIR 7628 security requirements.		
MIL3	i. The performance of the cybersecurity program is monitored to ensure it aligns with the cybersecurity program strategy	There are no applicable NISTIR 7628 security requirements.		
	j. The cybersecurity program is independently reviewed (i.e., by reviewers who are not in the program) for achievement of cybersecurity program objectives	There are no applicable NISTIR 7628 security requirements.		
	k. The cybersecurity program addresses and enables the achievement of regulatory compliance as appropriate	SG.PM-1	GRC	Examine, Interview
	l. The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives	There are no applicable NISTIR 7628 security requirements.		

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
3. Establish and Maintain Cybersecurity Architecture				
MIL1	a. A strategy to architecturally isolate the organization’s IT systems from OT systems is implemented	SG.AC-5	UTR	Examine, Test
		SG.AC-19	CTR	Examine, Test
		SG.SC-7	UTR	Examine, Interview, Test
MIL2	b. A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy	SG.AC-5	UTR	Examine, Test
		SG.AC-19	CTR	Examine, Test
		SG.CP-7	GRC	Examine
		SG.CP-8	GRC	Examine, Interview
		SG.PE-11	GRC	Examine, Interview
		SG.SC-3	UTR	Examine, Test
		SG.SC-5	UTR	Examine, Test
		SG.SC-7	UTR	Examine, Interview, Test
		SG.SC-18	CTR	Examine, Interview
		SG.SC-20	CTR	Examine, Test
	c. Architectural segmentation and isolation is maintained according to a documented plan	SG.AC-5	UTR	Examine, Test
		SG.SC-7	UTR	Examine, Interview, Test
		SG.SC-18	CTR	Examine, Interview
MIL3	d. Cybersecurity architecture is updated at an organization-defined frequency to keep it current	SG.AC-5	UTR	Examine, Test
		SG.AC-19	CTR	Examine, Test
		SG.SC-7	UTR	Examine, Interview, Test
4. Perform Secure Software Development				
MIL1	No practice at MIL 1			
MIL2	a. Software to be deployed on assets that are important to the delivery of the function is developed using secure software development practices	There are no applicable NISTIR 7628 security requirements.		
MIL3	b. Policies require that software that is to be deployed on assets that are important to the delivery of the function be developed using secure software development practices	There are no applicable NISTIR 7628 security requirements.		
5. Management Activities				
MIL1	No practice at MIL 1			

Table A-1 (continued)
ES-C2M2 and NISTIR 7628 Security Requirements

ES-C2M2		NISTIR 7628	Requirement Type	NISTIR 7628 Assessment Method
Risk Management				
MIL2	a. Documented practices are followed for cybersecurity program management activities	SG.PM-2	GRC	Examine, Interview
	b. Stakeholders for cybersecurity program management activities are identified and involved	SG.PM-2	GRC	Examine, Interview
	c. Standards and/or guidelines have been identified to inform cybersecurity program management activities	There are no applicable NISTIR 7628 security requirements.		
MIL3	d. Cybersecurity program management activities are guided by documented policies or other organizational directives	SG.AC-1 SG.AU-1 SG.PL-5 SG.PM-1 SG.PM-2	GRC GRC GRC GRC GRC	Examine, Interview Examine, Interview Examine, Interview Examine, Interview Examine, Interview
	e. Cybersecurity program management activities are periodically reviewed to ensure conformance with policy	SG.PM-2	GRC	Examine, Interview
	f. Personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities	There are no applicable NISTIR 7628 security requirements.		

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

3002003332

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