Guide to the Distributed Energy Resources Cybersecurity Framework

Charisa Powell, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-75044
December 2019

Guide to the Distributed Energy Resources Cybersecurity Framework

Charisa Powell, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds

National Renewable Energy Laboratory

Suggested Citation
Powell, Charisa, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds. 2019. *Guide to the Distributed Energy Resources Cybersecurity Framework*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-75044. https://www.nrel.gov/docs/fy20osti/75044.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-75044
December 2019

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

Acknowledgments

This material is based on work supported by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy (EERE) Federal Energy Management Program.

The authors thank EERE Energy Technology Program Specialist Saralyn Bunch for her support and oversight throughout the project. Additionally, the authors thank the U.S. General Services Administration's Denver Federal Center facilities manager, the Naval Base San Diego Energy Management Team, and the National Renewable Energy Laboratory's facility managers for their cooperation in allowing our research team to study the security posture of their premises and operations.

Principal Investigator
Tami Reynolds

Web Tool Architects
Matt McDaniel

Joshua Van Natta

List of Acronyms

AAA	Authentication, Authorization, and Accounting
ES- C2M2	Electric Sector Cybersecurity Capability Maturity Model
COP	common operating picture
DER	distributed energy resource
DERCF	Distributed Energy Resource Cybersecurity Framework
DOE	U.S. Department of Energy
EDM	Enterprise Data Management
EERE	Office of Energy Efficiency and Renewable Energy
EV	electric vehicle
ICS	industrial control systems
IT	information technology
kWh	kilowatt-hour
MW	megawatt
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
PV	photovoltaic
SANS Institute	System Administration, Networking, and Security Institute

Executive Summary

In May 2018, the U.S. Department of Energy (DOE) released its Cybersecurity Strategy (DOE 2018), a multiyear plan specifically regarding cybersecurity in the energy sector. The framework outlined in this report aligns with strategies identified in the DOE cybersecurity strategy to deliver cybersecurity solutions and continually improve cybersecurity posture. Researchers from federal facilities and industry can now make use of this framework, the Distributed Energy Resources Cybersecurity Framework (DERCF), through a web-based application. The application presents users with questions regarding their organization's security controls, practices pertaining to the use of such controls, and application to distributed energy resources (DERs) in the following categories:

- Cyber governance
- Cyber-physical technical management
- Physical security of DER devices.

DERs contribute to increased connectivity within energy systems and their components, thus increasing the attack surface that a threat actor can target. A standardized procedure to assess DER cybersecurity falls behind the rapid pace of DER adoption. The DERCF web application will draw from users' responses to generate a score that gauges the current state of DER cybersecurity in organizations and prioritizes recommended action items to help improve an organization's security controls and practices.

Input, calculation, presentation, and optional storage of data through the DERCF web application will be handled securely in compliance with the National Institute of Standards and Technology Special Publication 800-53.

This document provides an overview of the DERCF and serves as a guide to applying this framework to DERs. It also provides guidance on a method to conduct a cybersecurity assessment, using the controls presented in Appendix A.

Table of Contents

List of Figures

List of Tables

1 Introduction

With increased deployment of distributed energy resources (DERs) comes the critical responsibility of securing them. Securing systems that have high penetration of DERs will require a multifaceted approach to cybersecurity that must be addressed at every level, from individual components to system architecture.

DERs can be found in a variety of settings, including, but not limited to, federal sites and residential areas. Compared to the traditional electric grid that is powered by a relatively small number of large, centralized generation facilities, modern generation and distribution systems are becoming increasingly reliant on smaller decentralized generation sources. The transition to an energy system that relies on such resources requires careful coordination by operators to maintain stability.

Further complications arise from the significant and increasing portions of DERs owned and controlled by consumers and third parties, who might not be aware of the need for robust cybersecurity. Although smart meters and advanced metering infrastructure have already expanded utilities' attack surfaces, increased deployment of DERs presents additional risks because of (1) their distributed topology, (2) their control and communications requirements, and (3) the large number of distribution-side devices and accompanying access points that operate outside utilities' administrative domains.

Although DERs fall under the umbrella of industrial control systems (ICS), they pose additional unique cybersecurity challenges. Lack of flexibility and visibility into ICS can create an environment where adversarial movement goes undetected. Further, DERs represent a burgeoning technology area that is expanding to include smart systems technology.

The Distributed Energy Resources Cybersecurity Framework (DERCF) builds on the Electric Sector Cybersecurity Capability Maturity Model (ES-C2M2), which was developed by the U.S. Department of Energy (DOE 2014) in collaboration with the U.S. Department of Homeland Security. Specifically, the DERCF adopts controls from the ES-C2M2's governance-oriented document and creates two additional domains mirroring the ES-C2M2 language. Federal agencies are required by Executive Order 13800 to use The Framework for Improving Critical Infrastructure Cybersecurity (The Framework), developed by the National Institute of Standards and Technology (NIST), or any successor document, to manage the agency's cybersecurity risk ("Executive Order 13800"). Appendix A maps the relationship between the DERCF and The Framework to provide reference to additional controls.

1.1 Purpose of This Guide

This document is intended to provide an overview of cybersecurity risk as it relates directly to DERs. In addition to serving as a detail-oriented reference regarding cybersecurity controls for DERs, this document provides guidance on how to use the web-based tool for maximum benefit.

1.1.1 Intended Audience and Users

This guide is intended for those who plan to assess and improve the cybersecurity posture of their organizations, including, but not limited to, federal, private, and utility sites that have

DERs. Because the DERCF is a public-facing web tool, it is open for anyone to create an account and take an assessment based on their DER information.

1.1.2 Use of the Guide

Although this document can be used independently of the web-based tool (because it lists the controls that define the framework), it does not include an automatic scoring system or the associated action items generated from the online assessment algorithm. We recommend using this report as a complement to the web-based tool, which does offer an automatic scoring system.

Section 2 explains the various project components, including a survey of relevant research and the state-of-the-art. Section 3 details the organization and structure of the DERCF. Documentation for how to use the DERCF web tool can be found on NREL's website at no cost. Appendix A comprises a list of the framework's controls, categorized by domain.

1.2 Background

To address the challenges of DER cybersecurity, researchers at the National Renewable Energy Laboratory (NREL) developed a holistic DER cybersecurity framework that includes a tool for evaluating the cybersecurity posture of federal sites that already employ distributed energy resource (DER) systems or plan to implement DERs to support daily operations.

Designed to identify and target security risks that DERs pose to the local grid and beyond, NREL's DERCF covers the following classifications:

- Solar photovoltaic (PV) generation
- Wind energy generation
- Electric vehicle (EV) charging stations
- Distributed energy storage systems.

The DERCF is based on three pillars: governance, technical management, and physical security, described later in this document. These pillars use current standards as a reference for assessment questions, with flexibility for future improvements. Flexibility of the tool is critical because each DER site is different, but the desire to adhere to best practices is consistent.

Simple misconfigurations of DER systems can contribute to extreme vulnerabilities because the connectivity of DERs creates a higher risk for scaled attacks that extend past local resources and into the energy system. The technical management pillar focuses directly on settings and procedures related to system operation. Similarly, a lapse in the proper implementation of physical security assets and procedures of a site can allow malicious access to high-priority assets.

The DERCF is an evaluation that can be taken repeatedly by any organization that aims to measure cybersecurity maturity levels over time. Additionally, it provides a reference point for sites that are required to achieve authority to operate.

1.2.1 DER Systems

The large-scale nature of DER systems dictates a hierarchical approach to controlling them. Recognizing the distinctions among all five levels (depicted in Figure 1) is important to

comprehensively understanding DER systems from a security standpoint; however, the DERCF focuses specifically on Level 1 and Level 2, which are primarily concerned with physical DER devices and the immediate systems that control them.

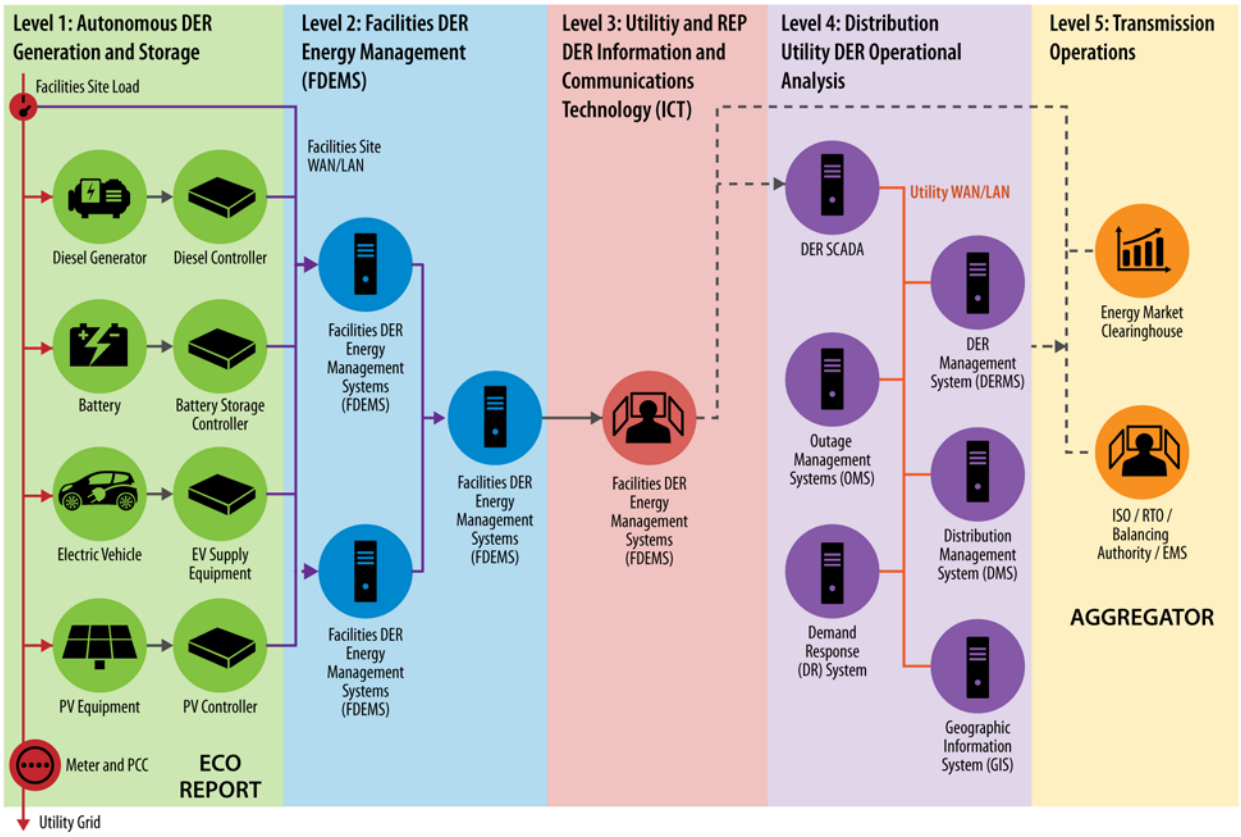

Figure 1. DER system architecture

***Illustration by Alfred Hicks, NREL*. Source: Cleveland and Lee (2013)[1]**

Level 1—Autonomous DER Generation and Storage: The DERCF assesses the independently functioning DER devices within Level 1 (e.g., PV arrays, wind turbines, and charging stations) on a technical level, based on responses to questions specific to communications protocols, patching techniques, and other system configuration elements. It is here—where the tangible devices, assets, and hardware are present—that physical security is paramount, requiring attention to detail and thorough implementation.

Level 2—Facilities DER Energy Management System: The DERCF also takes into consideration a wider scope of the DER site with a sitewide physical security assessment focused on the cyber-physical systems. Additionally, it includes a deep look at account management procedures of the facility DER management system as well as the cybersecurity posture of the internal local area network.

[1] The research was produced by the Electric Power Research Institute and paid for by the U.S. Department of Energy (DOE) under the National Electric Sector Cybersecurity Organization Resource grant DE-OE0000524.

1.2.2 Common Vulnerabilities and Previous Attacks

In addition to the increasing adoption of renewables, current global events pertaining to the cybersecurity of ICS have increased the urgency to incorporate cyber best practices. In 2010, the Stuxnet worm became the first cybersecurity attack targeting ICS. Using a zero-day vulnerability, the malicious software stealthily navigated Windows machines with the intent to cause physical destruction. By infecting targeted programmable logic controllers, the malware caused equipment to run at speeds outside the scope of normal operation (Mueller and Yadegari 2012).

In a more recent event, a cyberattack on the Ukrainian power grid (SANS 2016) demonstrated the potential scale of a cyber event by cutting off power from more than 200,000 customers. On a technical level, this attack used a combination of spear phishing, remote-access vulnerabilities, and firmware modification to render physical systems inoperable and cause major power outages.

Work by Sebastian and Hahn (2017) presented findings from extensive research on a consequence-based level for misconfigured DER systems. These systems were assigned to various attack scales, including individual DERs, local neighborhoods, and distribution/transmission systems. For each attack scale, a vulnerable grid-support function (such as frequency adjustments and islanding detection) was identified, along with the potential consequences. This research played an important role in cyber risk management of DERs, and it guided the formation of the DERCF's three pillars.

1.2.3 Relevant Research

Although cybersecurity in general has been a growing concern for all industries for the past decade, in some cases DERs have introduced new risks in areas that are not always applicable to the information technology (IT) world. The lack of built-in security and use of unique communications protocols set DERs apart. Development of the DERCF was influenced by technical work by Darwish et al. (2015), Miranda and Goldsmith (2017), and Sebastian and Hahn (2017), which considered the categorization of cyberattacks on DER systems.

The security mechanisms and controls that shape the domains of the framework directly align with the guidelines for confidentiality, integrity, and availability, presented by the National Institute of Standards and Technology (NIST).

The technical management and physical pillars of the DERCF provide controls and recommendations based on the following standards and frameworks:

- NIST SP 800-53, SP 800-30, SP 800-82, SP 800-37, SP 800-63B, NISTIR 7628, NIST Cybersecurity Framework
- U.S. Department of Homeland Security Cybersecurity Assessment for Industrial Control Systems, Seven Steps to Effectively Defend Industrial Control Systems
- Interagency Security Committee Security Specialist Competencies, Interagency Security Committee Best Practices for Planning and Managing Physical Security Resources

- U.S. Department of Defense Education Activity Physical Security & Antiterrorism, International Electrotechnical Commission Technical Report 62351, Cybersecurity for Distributed Energy Resources
- Executive Order 13800
- Cybersecurity for DER Systems
- Cybersecurity Procurement Language for Energy Delivery Systems
- Institute of Electrical and Electronics Engineers 2030.5 and California Rule 21.

1.2.4 The Growth of DERs

A major hurdle for the solar power industry has been the cost of installation and operation of PV. During the past few years, research efforts have effectively made PV cheaper and more reliable as an energy source. DOE has set a nationwide goal to reduce the cost of residential solar PV to $.05/kilowatt-hour (kWh), while reducing the cost of utility-scale PV to $.03/ kWh by 2030.[2] With this significant reduction, the penetration level of solar power in the United States is expected to skyrocket, especially in residential areas. For example, the Hawaiian Electric Company anticipates that renewable energy sources (e.g., solar, wind) will account for 100% of its net electricity generation by 2045 (NREL 2018).

Similarly, wind energy continues to grow rapidly. In just one year, more than 8,200 megawatts (MW) of capacity were added in the United States (DOE 2017). Not only does this significantly reduce the burden on other forms of power generation, but it also increases the opportunity for the integration of energy systems. the opportunity for the integration of energy systems.

A forward-thinking consideration is the role EVs will play in the future because research is still developing to tie EV batteries to grid stability. For context on how expansive EVs are becoming: of the total number of EV charging stations that will be needed to support America by 2025, only 25% have been installed (Nicholas 2019). This number is more significant in states where the demand is more concentrated.

1.2.5 Physical Controls and Cybersecurity

Although it might seem unrelated at a high level, the physical security of DERs is critical to managing the cybersecurity risk of all assets. Physical access to a system responsible for controlling operational technology would bypass and undermine the complex and expensive cybersecurity barriers designed to keep remote attackers out of a system. Strong physical controls aid in the mitigation of social engineering, insider threats, and neglected best practices, because humans are often the weakest link in security.

All DERCF assessment questions under the physical security pillar are based on observations from federal site visits, physical security control best-practice documentation, as well as the System Administration, Networking, and Security (SANS) Institute's physical security specialist training. These questions are designed to be applied sitewide because elevated access to a site or facility in which the DERs are housed can have equally significant, if not more severe,

[2] This goal refers to the unsubsidized, levelized U.S. average for commercial and residential rooftop PV (SunShot 2016).

implications than threats that originate from remote and unauthorized access to the controls of DERs alone.

Further, the human component is a major aspect of system security and is historically the weakest link in holistic security postures. In the scope of DERs, the human component spans multiple entities, including, but not limited to, the utility, site operation, and manufacturers. Because DERs represent a transitional energy solution, standards regulating physical security and access controls to data are limited.

Figure 2 shows a graphic representation of the physical security layers that separate unauthorized users from different levels of access to any given site or facility and its controls.

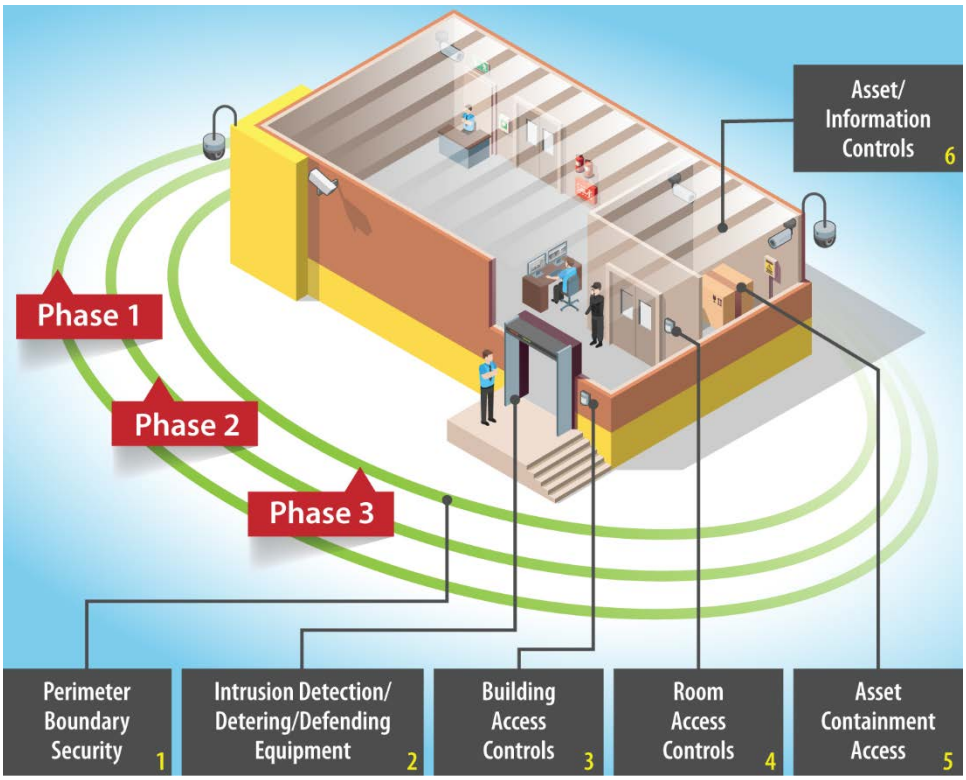

Figure 2. Physical security layers

Illustration by Alfred Hicks, NREL

Five levels isolate the exterior of a given facility, and traditionally this is how the progression of an in-person physical security assessment would be conducted. The phases represent the three levels of perimeter boundary security: phase one represents fixed-perimeter assets like fences; phase two represents smart assets that alert to one or more physical security specialists who work for the site; and phase three represents guards that monitor and operate the other two phases of perimeter access.

As with any type of assessment, there are many elements where a question-based approach is not as comprehensive as an onsite assessment. The DERCF overcomes the lack of an in-person audit of physical security implementations by applying generalized physical security control questions that can be applied to a variety of site configurations. This method of assessing comes from the

SANS Institute's physical security specialist training and looks at the perimeter boundary, intrusion-detection equipment, building access controls, room access controls, and asset containment access controls, starting from layer one and ending at layer five (The CORE Group 2019). The DERCF approach is like planning a security posture with phase lines that act as single points of failure, also known as defense in-depth.

1.2.6 Value Added

Intended to extend the implementation of ES-C2M2, the DERCF project also provides:

- An extension to technical and physical components related to DERs and their respective cybersecurity needs
- An interactive, web-based tool to guide the cybersecurity assessment process
- A digitally generated report with a custom scoring system and prioritized action items.

NREL evaluated DOE's ES-C2M2 and other existing cybersecurity assessment tools to establish a benchmark based on previous work. The results reveal that such tools do not provide sufficient guidance for users to understand and fully address cybersecurity vulnerabilities of DER systems. To bridge the gap, the work described in this document aims to help federal agencies address deficiencies in their cybersecurity postures that create vulnerabilities in their DER systems, which they might not otherwise know exist.

2 Core Concepts

This section addresses details of the project as well as components of the web application and its features at a high level.

2.1 Methodology

Although there is no comprehensive list of controls that ensures perfect security, efforts in the DERCF project are heavily focused on creating a holistic and flexible framework. The following tasks were executed:

1. Performed initial discovery assessments at federal sites (including both NREL campuses) to better understand DER integration, requirements, and operations and to gather user feedback
2. Reviewed and refined DERCF content, such as questions and resources, to ensure that the framework is comprehensive and complete
3. Categorized assessment questions by appropriate domains and subdomains
4. Designed and implemented the public web application to encompass areas of project research
5. Created an optional internal administrator portal to access assessment metadata for ongoing research by NREL. Federal data cannot be stored or used in any way by NREL or any other organization without case-by-case permission of the user.

To identify common trends in cybersecurity practices and help create a more streamlined process for all sites with DERs, the administrator portal serves as a critical source of information to be used in further research at NREL.

2.2 Technical Approach to the Tool

This section provides details on the functionality of the web application.

2.2.1 Preliminary Assessment

The preliminary assessment provides an opportunity for users to identify and document the types of DERs their site has in operation. Users can specify the type of DER (e.g., wind, PV), device manufacturer, and generation capacity.

2.2.2 Roles

All roles are defined to help determine which users are the most appropriate to accurately answer certain types of questions. These include:

- **Energy systems manager:** management-level individual responsible for overseeing a team of technical personnel in the field of energy systems
- **Systems/controls engineer:** technical individual primarily working directly with control systems for research and/or operational purposes
- **Site security manager:** management-level individual overseeing sitewide physical-security personnel and site operations

- **DER system administrator:** network/system administrator for the DER system (and, in some cases, also the IT/operational system)
- **Technology (operational technology) system administrator:** individual responsible for managing accounts and system configuration
- **Compliance officer:** individual responsible for enforcing up-to-date standards relevant to DERs (note that this role can overlap with any other role)
- **Information technology personnel:** individual(s) responsible for procuring, maintaining, and securing information technology components
- **Human resources personnel:** sitewide team specifically assigned to administrative tasks related to employees
- **Manufacturer:** external/third-party hardware manufacturer for DER devices and their components.

Note that these roles do not constitute an exhaustive list of personnel a site might have. Additionally, some roles may be combined into a single individual.

2.2.3 Assessment

The assessment, the core of the online tool's functionality, comprises questions organized by domain and sectioned by subdomain. Each section of the assessment can be accessed from the customized dashboard that serves as the user interface for the tool. The tool allows users to save in-progress assessments and resume work later.

2.2.4 Report and Scoring

An official score, prioritized list of action items, and other pertinent information about cybersecurity posture are available in the report section within the tool.

To provide a score at a glance, accompanied by a custom, prioritized list of action items, the DERCF uses different algorithms to quantify the cybersecurity posture in the three model pillars (governance, technical, and physical security), which are further detailed in Section 3. The governance pillar, based on ES-C2M2, is scored on a maturity level where the available responses are consistent for all questions. The maturity levels are:

- Not implemented
- Limited (i.e., concepts have been casually discussed)
- Documented
- Documented and shared
- Documented and shared, with training available.

With a more complex scoring system than that of the ES-C2M2-based governance pillar, the technical management pillar can include follow-up questions that invite more dynamic answers. It will consider user input, or the way the questions are answered, along with weighted values (based on their importance to the DER system as a whole) assigned to the questions. Together, these customized factors affect the score for the technical management pillar and provide a more accurate representation of the cybersecurity posture of their DERs.

Upon completion of an assessment, the user receives three scores (one for each domain), which can be combined into one overall score, similar to a standardized test score. The tool then automatically generates a list of prioritized, actionable intelligence items with resources mapped out to assist with implementing the controls. This prioritization is based on fundamental controls and procedures that must be in place to develop a stronger cybersecurity posture.

There is no limit to the number of assessments a user can perform. On the dashboard, users can see changes in their cybersecurity posture over time, depicted with graphs and other quantitative visualizations.

3 Model Pillars and Respective Domains

The DERCF's three foundational pillars—governance, technical management, and physical security—include several subdomains that further categorize assessment questions, making it easier to identify the correct personnel to answer them.

Each domain includes a purpose statement, which is a high-level summary of the domain's intent, followed by introductory notes that give context for the domain and introduce its practices.

Cyber Governance Security Assessment	Cyber-Physical Technical Management Security Assessment	Physical Security Assessment
Domains:	Domains:	Domains:
• Risk Management • Asset, Change, and Configuration • Identity and Access Management • Threat and Vulnerability Management • Situational Awareness • Information Sharing and Communication Management • Incident Response • External Dependency Management • Cybersecurity Program Management	• Account Management - Role-Based Access Control - Anomalous behavior in system logs • Configuration Management - Access Restrictions - Configuration Settings - Configuration Change Control - Internal/External User Management • Systems/Device Management - Fail-Safe Procedures - Ports and Input/output Device Access - Cryptographic Protection - Software Integrity/Patch Management	• Administration Controls - Audits - Holistic Security/Contingency Planning - Personnel Security Planning • Asset Controls - Equipment - Maintenance • Structure Controls - Distancing Practices for Sensitive Assets - Intrusion Detection/Prevention Assets - Response Teams/Force Protection

Figure 3. The DERCF's three domains and their respective subdomains address a comprehensive set of controls for securing DER technologies.

3.1 Governance

Each of the DERCF's 10 governance domains described comprises a structured set of cybersecurity practices for governance and does not deviate from the ES-C2M2, because these domains have already been carefully researched, validated, and consensually accepted as industry standard. The governance domains target the cyber policies of a site, and the following subsections (Sections 3.1.1 to 3.1.10) are taken directly from the DOE ES-C2M2 document. Primarily, assessment questions are geared toward information technology administrators, managers, and human resources departments. Topics of concern include documentation strategies as well as risk and threat management.

3.1.1 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.

3.1.2 Asset, Change, and Configuration Management

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

3.1.3 Identity and Access Management

Create and manage identities for entities that might 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.

3.1.4 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.

3.1.5 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.

3.1.6 Information Sharing and Communication

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

3.1.7 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.

3.1.8 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.

3.1.9 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.

3.1.10 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.

3.2 Cyber-Physical Technical Management

This domain contains practices/polices that extend the governance domain and are directly related to the operation of the systems. More specifically, this domain is focused on preserving the confidentiality, integrity, and availability of data traveling within a DER system and abroad.

3.2.1 Account Management

Establish and maintain a secure strategy that considers the role of the utility, site operator, and any other parties that might have access to the DER system. Further, ensure periodic review of the strategy, making adjustments as systems and roles change.

3.2.2 System and Device Management

Manage and maintain a site's hardware and software devices as well as their controlling systems. This includes patch management, cryptographic and data integrity settings, and fail-safe procedures.

3.2.3 Configuration Management

Establish and maintain a resilient system through firewall rules, timeout settings, and other configurable settings that directly relate to DER systems.

3.3 Physical Security

The physical security subdomains and relevant controls are independent of the cybersecurity governance and technical subdomains. These controls are applicable sitewide as well as to components that specifically touch the DER system.

3.3.1 Administrative Controls

Establish and maintain a standard procedure for managing audits, prioritizing major areas of concern, and planning/establishing procedures for all site operations.

3.3.2 Asset Controls

Develop procedures for routine maintenance of the DER system and site as a whole. Includes logging of performed maintenance to ensure the continuation of safe, secure, and efficient operations. Establish and maintain procedures for ensuring the safety of hardware, acquisition, delivery, and removal of assets, as well overall system design.

3.3.3 Structure Controls

Establish and maintain perimeter security, including, but not limited to, fences, door/gate locking, and controlled access areas (if applicable). This also encompasses monitoring the premises and surrounding areas.

4 Summary

DERs are increasingly prevalent in our energy systems. The DERCF is a framework available to federal sites, utility companies, and the general public to assess cybersecurity posture using a web-based tool. It is intended to serve as a first step to more broadly incorporating DERs into the cybersecurity conversation. As a continually evolving model and tool, the DERCF is designed with the inherent flexibility to grow and adapt to the changing world of DERs. Future work on this project includes expanded functionality of the web tool as well as updates to controls based on new standards, research, and user feedback.

Appendices of this document provide the controls from all pillars as a point of reference.

Glossary

Term	Definition
Attack scale	Surface area of a cascading cyberattack event on a system
Attack surface	Area most likely to be used by the attacker to initiate attacks
Authority to operate	Permission for a system/technology to be used under controlled and/or accepted risk
Common operating picture	Organization's single place to process information for business operations
Decentralized generation	Generation of electricity by small and distributed energy resources
DER penetration	A measure of distributed energy resource generation within a system
Facility DER management system	Centralized management system to control, monitor, and maintain distributed energy resource operations
Fail-safe procedure	A method that is triggered in the event of unexpected behavior to prevent equipment damage
Grid edge	End devices usually placed at properties that are connected to the grid
Grid stability	Normal operation of the grid
Islanding protection	Protection of distributed generator-powered location when connection to the grid is lost
Programmable logic controller	An industrial computer that automates electrical processes
Red teaming	Testing an equipment, network, or a system by exploiting it for the purpose of improving it
Single point of failure	A particular part of the system that would stop operations entirely if its functionality were compromised
Spear phishing	The practice of sending unsolicited emails to targeted individuals that appear to be from a trusted sender to compromise information

References

Cleveland, Frances, and Annabelle Lee. 2013. “Cybersecurity for DER Systems.” Electric Power Research Institute. http://smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf.

The CORE Group. "SANS Physical Security Specialist." Lecture 1, Austin, Texas, May 10, 2019.

Darwish, Ihab, Obinna Igbe, Orhan Celebi, Tarek Saadawi, and Joseph Soryal. 2015. “Smart Grid DNP3 Vulnerability Analysis and Experimentation.” 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, 2015. https://doi.org/10.1109/CSCloud.2015.86.

DOE. 2014. “Electric Sector Cybersecurity Capability Maturity Model (ES-C2M2).” Energy.gov. https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

DOE. 2017. “Energy Department Reports: Wind Energy Continues Rapid Growth in 2016.” Energy.Gov. https://www.energy.gov/articles/energy-department-reports-wind-energy-continues-rapid-growth-2016.

DOE. 2018. "Cybersecurity Strategy." Energy.gov.

https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf.

“Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.” Code of Federal Regulations, title 3 (2017 comp.). https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Miranda, A. W., and S. Goldsmith. 2017. “Cyber-Physical Risk Management for PV Photovoltaic Plants.” In 2017 International Carnahan Conference on Security Technology (ICCST), 1–8. https://doi.org/10.1109/CCST.2017.8167813.

Mueller, Paul, and Babak Yadegari. 2012. “The Stuxnet Worm.” https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf.

National Renewable Energy Laboratory. 2018. “NREL and Hawaiian Electric Navigate Uncharted Waters of Energy Transformation (Part 2) | News | NREL.” https://www.nrel.gov/news/features/2018/nrel-and-hawaiian-electric-navigate-uncharted-waters-of-energy-transformation-part-2.html.

SANS. 2016. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” SANS ICS. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Sebastian, D. J., and A. Hahn. 2017. “Exploring Emerging Cybersecurity Risks from Network-Connected DER Devices.” In 2017 North American Power Symposium (NAPS), 1–6. https://doi.org/10.1109/NAPS.2017.8107267.

Appendix A. Assessment Controls

This section contains a list of the controls that can be found in the online assessment.

A.1 Cybersecurity Governance

The table below lists objectives from the ES-C2M2 document, along with the associated domains and subdomains. For more information on the controls referenced by their unique notation (for example, RM-2f), see the ES-C2M2 document. Recall that these objectives are assessed based on a maturity level ranging from "not implemented" to "documented, shared, and updated." The requirements of these controls are inclusive of the NIST Cybersecurity Framework and focus on utilities and their DERs.

Table A.1. Cybersecurity Governance

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Risk Management	Establish Cybersecurity Risk-Management Strategy	There is a documented cybersecurity risk-management strategy.	Identify
Risk Management	Establish Cybersecurity Risk-Management Strategy	The strategy provides an approach for risk prioritization, including consideration of impact.	Identify
Risk Management	Establish Cybersecurity Risk-Management Strategy	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.	Identify
Risk Management	Establish Cybersecurity Risk-Management Strategy	The risk-management strategy is periodically updated to reflect the current threat environment.	Identify
Risk Management	Establish Cybersecurity Risk-Management Strategy	An organization-specific risk taxonomy is documented and used in risk-management activities.	Identify
Risk Management	Establish Cybersecurity Risk-Management Strategy	Cybersecurity risks are identified.	Identify
Risk Management	Manage Cybersecurity Risk	Identified risks are mitigated, accepted, tolerated, or transferred.	Identify
Risk Management	Manage Cybersecurity Risk	Risk assessments are performed to identify risks in accordance with the risk-management strategy.	Identify
Risk Management	Manage Cybersecurity Risk	Identified risks are documented.	Identify
Risk Management	Manage Cybersecurity Risk	Identified risks are analyzed to prioritize response activities in accordance with the risk-management strategy.	Identify; Protect
Risk Management	Manage Cybersecurity Risk	Identified risks are monitored in accordance with the risk-management strategy.	Identify
Risk Management	Manage Cybersecurity Risk	Risk analysis is informed by network (IT and/or OT) architecture.	Identify
Risk Management	Manage Cybersecurity Risk	The risk-management program defines and operates risk-management policies and procedures that implement the risk-management strategy.	Identify
Risk Management	Manage Cybersecurity Risk	A current cybersecurity architecture is used to inform risk analysis.	Identify
Risk Management	Manage Cybersecurity Risk	A risk register (a structured repository of identified risks) is used to support risk-management activities.	Identify; Protect; Respond
Risk Management	Manage Cybersecurity Risk	Documented practices are followed for risk-management activities.	Identify
Risk Management	Management Activities	Stakeholders for risk-management activities are identified and involved.	Identify
Risk Management	Management Activities	Adequate resources (people, funding, and tools) are provided to support risk-management activities.	Identify
Risk Management	Management Activities	Standards and/or guidelines have been identified to inform risk-management activities.	Identify
Risk Management	Management Activities	Risk-management activities are guided by documented policies or other organizational directives.	Identify
Risk Management	Management Activities	Risk-management policies include compliance requirements for specified standards and/or guidelines.	Identify

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Risk Management	Management Activities	Risk-management activities are periodically reviewed to ensure conformance with policy.	Identify
Risk Management	Management Activities	Responsibility and authority for the performance of risk-management activities are assigned to personnel.	Identify
Risk Management	Management Activities	Personnel performing risk-management activities have the skills and knowledge needed to perform their assigned responsibilities.	Identify
Asset, Change, and Configuration Management	Manage Asset Inventory	There is an inventory of IT and OT assets that are important to the delivery of the function.	Identify
Asset, Change, and Configuration Management	Manage Asset Inventory	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).	Identify
Asset, Change, and Configuration Management	Manage Asset Inventory	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).	Identify
Asset, Change, and Configuration Management	Manage Asset Inventory	Inventoried assets are prioritized based on their importance to the delivery of the function.	Identify
Asset, Change, and Configuration Management	Manage Asset Inventory	There is an inventory for all connected IT and OT assets related to the delivery of the function.	Identify
Asset, Change, and Configuration Management	Manage Asset Inventory	The asset inventory is current (as defined by the organization).	Identify
Asset, Change, and Configuration Management	Manage Asset Configuration	Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly.	Protect
Asset, Change, and Configuration Management	Manage Asset Configuration	Configuration baselines are used to configure assets at deployment.	Protect
Asset, Change, and Configuration Management	Manage Asset Configuration	The design of configuration baselines includes cybersecurity objectives.	Protect
Asset, Change, and Configuration Management	Manage Asset Configuration	Configuration of assets is monitored for consistency with baselines throughout the assets' life cycle.	Protect
Asset, Change, and Configuration Management	Manage Asset Configuration	Configuration baselines are reviewed and updated at an organizationally defined frequency.	Protect
Asset, Change, and Configuration Management	Manage Change to Assets	Changes to inventoried assets are evaluated before being implemented.	Protect
Asset, Change, and Configuration Management	Manage Change to Assets	Changes to inventoried assets are logged.	Protect
Asset, Change, and Configuration Management	Manage Change to Assets	Changes to assets are tested prior to being deployed, whenever possible.	Protect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Asset, Change, and Configuration Management	Manage Change to Assets	Change-management practices address the full life cycle of assets (i.e., acquisition, deployment, operation, and retirement).	Protect
Asset, Change, and Configuration Management	Manage Change to Assets	Changes to assets are tested for cybersecurity impact prior to being deployed.	Protect
Asset, Change, and Configuration Management	Manage Change to Assets	Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality).	Protect
Asset, Change, and Configuration Management	Management Activities	Documented practices are followed for asset inventory, configuration, and change-management activities.	Protect
Asset, Change, and Configuration Management	Management Activities	Stakeholders for asset inventory, configuration, and change-management activities are identified and involved.	Protect
Asset, Change, and Configuration Management	Management Activities	Adequate resources (people, funding, and tools) are provided to support asset inventory, configuration, and change-management activities.	Protect
Asset, Change, and Configuration Management	Management Activities	Standards and/or guidelines have been identified to inform asset inventory, configuration, and change-management activities.	Protect
Asset, Change, and Configuration Management	Management Activities	Asset inventory, configuration, and change-management activities are guided by documented policies or other organizational directives.	Protect
Asset, Change, and Configuration Management	Management Activities	Asset inventory, configuration, and change-management policies include compliance requirements for specified standards and/or guidelines.	Protect
Asset, Change, and Configuration Management	Management Activities	Asset inventory, configuration, and change-management activities are periodically reviewed to ensure conformance with policy.	Protect
Asset, Change, and Configuration Management	Management Activities	Responsibility and authority for the performance of asset inventory, configuration, and change-management activities are assigned to personnel.	Protect
Asset, Change, and Configuration Management	Management Activities	Personnel performing asset inventory, configuration, and change-management activities have the skills and knowledge needed to perform their assigned responsibilities.	Protect
Identity and Access Management	Establish and Maintain Identities	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).	Protect
Identity and Access Management	Establish and Maintain Identities	Credentials are issued for personnel and other entities who require access to assets (e.g., passwords, smart cards, certificates, keys).	Protect
Identity and Access Management	Establish and Maintain Identities	Identities are deprovisioned when no longer required.	Protect
Identity and Access Management	Establish and Maintain Identities	Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access).	Protect
Identity and Access Management	Establish and Maintain Identities	Credentials are periodically reviewed to ensure that they are associated with the correct person or entity.	Protect
Identity and Access Management	Establish and Maintain Identities	Identities are deprovisioned within organizationally defined time thresholds when no longer required.	Protect
Identity and Access Management	Establish and Maintain Identities	Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher-risk access) (RM-1c).	Protect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Identity and Access Management	Control Access	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).	Protect
Identity and Access Management	Control Access	Access is granted to identities based on requirements.	Protect
Identity and Access Management	Control Access	Access is revoked when no longer required.	Protect
Identity and Access Management	Control Access	Access requirements incorporate least-privilege and separation-of-duties principles.	Protect
Identity and Access Management	Control Access	Access requests are reviewed and approved by the asset owner.	Protect
Identity and Access Management	Control Access	Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring.	Protect
Identity and Access Management	Control Access	Access privileges are reviewed and updated to ensure validity at an organizationally defined frequency.	Protect
Identity and Access Management	Control Access	Access to assets is granted by the asset owner, based on risk to the function.	Protect
Identity and Access Management	Control Access	Anomalous access attempts are monitored as indicators of cybersecurity events.	Protect
Identity and Access Management	Management Activities	Documented practices are followed to establish and maintain identities and control access.	Protect
Identity and Access Management	Management Activities	Stakeholders for access and identity-management activities are identified and involved.	Identify; Protect
Identity and Access Management	Management Activities	Adequate resources (people, funding, and tools) are provided to support access and identity-management activities.	Protect
Identity and Access Management	Management Activities	Standards and/or guidelines have been identified to inform access and identity-management activities.	Protect
Identity and Access Management	Management Activities	Access and identity-management activities are guided by documented policies or other organizational directives.	Protect
Identity and Access Management	Management Activities	Access and identity-management policies include compliance requirements for specified standards and/or guidelines.	Protect
Identity and Access Management	Management Activities	Access and identity-management activities are periodically reviewed to ensure conformance with policy.	Protect
Identity and Access Management	Management Activities	Responsibility and authority for the performance of access and identity-management activities are assigned to personnel.	Protect
Identity and Access Management	Management Activities	Personnel performing access and identity-management activities have the skills and knowledge needed to perform their assigned responsibilities.	Protect
Threat and Vulnerability Management	Identify and Respond to Threats	Information sources to support threat-management activities are identified (e.g., United States Computer Emergency Readiness Team [US-CERT], various critical infrastructure sector Information Sharing and Analysis Centers [ISACs], Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], industry associations, vendors, federal briefings).	Identify
Threat and Vulnerability Management	Identify and Respond to Threats	Cybersecurity threat information is gathered and interpreted for the function.	Identify; Protect
Threat and Vulnerability Management	Identify and Respond to Threats	Threats considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status).	Identify; Protect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Threat and Vulnerability Management	Identify and Respond to Threats	A threat profile for the function is established that includes characterization of likely intent, capability, and target of threats to the function.	Identify; Protect; Detect; Respond; Recover
Threat and Vulnerability Management	Identify and Respond to Threats	Threat information sources that address all components of the threat profile are prioritized and monitored.	Identify; Protect
Threat and Vulnerability Management	Identify and Respond to Threats	Identified threats are analyzed and prioritized.	Identify
Threat and Vulnerability Management	Identify and Respond to Threats	Threats are addressed according to the assigned priority.	Protect
Threat and Vulnerability Management	Identify and Respond to Threats	The threat profile for the function is validated at an organization-defined frequency.	Identify; Protect
Threat and Vulnerability Management	Identify and Respond to Threats	Analysis and prioritization of threats are informed by the function's (or organization's) risk criteria (RM-1c).	Identify; Protect
Threat and Vulnerability Management	Identify and Respond to Threats	Threat information is added to the risk register (RM-2j).	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Information sources to support cybersecurity-vulnerability discovery are identified (e.g., US-CERT, various critical infrastructure sector ISACs, ICS-CERT, industry associations, vendors, federal briefings, internal assessments).	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity-vulnerability information is gathered and interpreted for the function.	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implementing mitigating controls, applying cybersecurity patches).	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity-vulnerability information sources that address all assets important to the function are monitored.	Identify; Protect; Detect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity-vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools).	Identify; Protect; Detect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	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).	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity vulnerabilities are addressed according to the assigned priority.	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Operational impact to the function is evaluated prior to deploying cybersecurity patches.	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity-vulnerability assessments are performed for all assets important to the delivery of the function at an organization-defined frequency.	Identify; Protect; Detect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity-vulnerability assessments are informed by the function's (or organization's) risk criteria (RM-1c).	Identify; Protect; Detect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity-vulnerability assessments are performed by parties that are independent of the operations of the function.	Identify; Protect; Detect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Analysis and prioritization of cybersecurity vulnerabilities are informed by the function's (or organization's) risk criteria (RM-1c).	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Cybersecurity-vulnerability information is added to the risk register (RM-2j).	Identify; Protect
Threat and Vulnerability Management	Reduce Cybersecurity Vulnerabilities	Risk-monitoring activities validate the responses to cybersecurity vulnerabilities (e.g., deployment of patches or other activities).	Identify; Protect
Threat and Vulnerability Management	Management Activities	Documented practices are followed for threat and vulnerability-management activities.	Identify; Protect
Threat and Vulnerability Management	Management Activities	Stakeholders for threat and vulnerability-management activities are identified and involved.	Identify; Protect
Threat and Vulnerability Management	Management Activities	Adequate resources (people, funding, and tools) are provided to support threat and vulnerability-management activities.	Identify; Protect
Threat and Vulnerability Management	Management Activities	Standards and/or guidelines have been identified to inform threat and vulnerability-management activities.	Identify; Protect
Threat and Vulnerability Management	Management Activities	Threat and vulnerability-management activities are guided by documented policies or other organizational directives.	Identify; Protect
Threat and Vulnerability Management	Management Activities	Threat and vulnerability-management policies include compliance requirements for specified standards and/or guidelines.	Identify; Protect
Threat and Vulnerability Management	Management Activities	Threat and vulnerability-management activities are periodically reviewed to ensure conformance with policy.	Identify; Protect
Threat and Vulnerability Management	Management Activities	Responsibility and authority for the performance of threat and vulnerability-management activities are assigned to personnel.	Identify; Protect
Threat and Vulnerability Management	Management Activities	Personnel performing threat and vulnerability-management activities have the skills and knowledge needed to perform their assigned responsibilities.	Identify; Protect
Situation Awareness	Perform Logging	Logging is occurring for assets important to the function where possible.	Protect
Situation Awareness	Perform Logging	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]).	Protect
Situation Awareness	Perform Logging	Log data are being aggregated within the function.	Protect
Situation Awareness	Perform Logging	Logging requirements are based on the risk to the function.	Protect
Situation Awareness	Perform Logging	Log data support other business and security processes (e.g., incident response, asset management).	Protect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Situation Awareness	Perform Monitoring	Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data).	Protect
Situation Awareness	Perform Monitoring	Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event.	Detect
Situation Awareness	Perform Monitoring	Monitoring and analysis requirements have been defined for the function and address timely review of event data.	Detect
Situation Awareness	Perform Monitoring	Alarms and alerts are configured to aid in the identification of cybersecurity events (IR-1b).	Detect
Situation Awareness	Perform Monitoring	Indicators of anomalous activity have been defined and are monitored across the operational environment.	Detect
Situation Awareness	Perform Monitoring	Monitoring activities are aligned with the function's threat profile (TVM-1d).	Detect
Situation Awareness	Perform Monitoring	Monitoring requirements are based on the risk to the function.	Detect
Situation Awareness	Perform Monitoring	Monitoring is integrated with other business and security processes (e.g., incident response, asset management).	Detect
Situation Awareness	Perform Monitoring	Continuous monitoring is performed across the operational environment to identify anomalous activity.	Detect
Situation Awareness	Perform Monitoring	Risk-register (RM-2j) content is used to identify indicators of anomalous activity.	Identify; Detect
Situation Awareness	Perform Monitoring	Alarms and alerts are configured according to indicators of anomalous activity.	Detect
Situation Awareness	Establish and Maintain a Common Operating Picture	Methods of communicating the current state of cybersecurity for the function are established and maintained.	Respond
Situation Awareness	Establish and Maintain a Common Operating Picture	Monitoring data are aggregated to provide an understanding of the operational state of the function (i.e., a common operating picture (COP); a COP may or may not include visualization or be presented graphically).	Protect; Detect
Situation Awareness	Establish and Maintain a Common Operating Picture	Information from across the organization is available to enhance the COP.	Protect
Situation Awareness	Establish and Maintain a Common Operating Picture	Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for the function to enhance the COP.	Protect; Detect
Situation Awareness	Establish and Maintain a Common Operating Picture	Information from outside the organization is collected to enhance the COP.	Protect; Detect
Situation Awareness	Establish and Maintain a Common Operating Picture	Predefined states of operation are defined and invoked (manual or automated process) based on the COP.	Protect; Detect
Situation Awareness	Management Activities	Documented practices are followed for logging, monitoring, and COP activities.	Protect; Detect
Situation Awareness	Management Activities	Stakeholders for logging, monitoring, and COP activities are identified and involved.	Protect; Detect
Situation Awareness	Management Activities	Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities.	Protect; Detect
Situation Awareness	Management Activities	Standards and/or guidelines have been identified to inform logging, monitoring, and COP activities.	Protect; Detect
Situation Awareness	Management Activities	Logging, monitoring, and COP activities are guided by documented policies or other organizational directives.	Protect; Detect
Situation Awareness	Management Activities	Logging, monitoring, and COP policies include compliance requirements for specified standards and/or guidelines.	Protect; Detect
Situation Awareness	Management Activities	Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy.	Protect; Detect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Situation Awareness	Management Activities	Responsibility and authority for the performance of logging, monitoring, and COP activities are assigned to personnel.	Protect; Detect
Situation Awareness	Management Activities	Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Information is collected from and provided to selected individuals and/or organizations.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Responsibility for cybersecurity reporting obligations is assigned to personnel (e.g., internal reporting, ICS-CERT, law enforcement).	Protect
Information Sharing and Communications	Share Cybersecurity Information	Information-sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected organizations, vendors, sector organizations, regulators, internal entities).	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Information is collected from and provided to identified information-sharing stakeholders.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Technical sources are identified that can be consulted on cybersecurity issues.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Provisions are established and maintained to enable secure sharing of sensitive or classified information.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Information-sharing practices address both standard operations and emergency operations.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Information-sharing stakeholders are identified based on shared interest in and risk to critical infrastructure.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	The function or the organization participates with information sharing and analysis centers.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Information-sharing requirements have been defined for the function and address timely dissemination of cybersecurity information.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	Procedures are in place to analyze and de-conflict received information.	Protect; Detect
Information Sharing and Communications	Share Cybersecurity Information	A network of internal and external trust relationships (formal and/or informal) has been established to vet and validate information about cyber events.	Protect; Detect
Information Sharing and Communications	Management Activities	Documented practices are followed for information-sharing activities.	Protect; Detect
Information Sharing and Communications	Management Activities	Stakeholders for information-sharing activities are identified and involved.	Protect; Detect
Information Sharing and Communications	Management Activities	Adequate resources (people, funding, and tools) are provided to support information-sharing activities.	Protect; Detect
Information Sharing and Communications	Management Activities	Standards and/or guidelines have been identified to inform information-sharing activities.	Protect; Detect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Information Sharing and Communications	Management Activities	Information-sharing activities are guided by documented policies or other organizational directives.	Protect; Detect
Information Sharing and Communications	Management Activities	Information-sharing policies include compliance requirements for specified standards and/or guidelines.	Protect; Detect
Information Sharing and Communications	Management Activities	Information-sharing activities are periodically reviewed to ensure conformance with policy.	Protect; Detect
Information Sharing and Communications	Management Activities	Responsibility and authority for the performance of information-sharing activities are assigned to personnel.	Protect; Detect
Information Sharing and Communications	Management Activities	Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities.	Protect; Detect
Information Sharing and Communications	Management Activities	Information-sharing policies address protected information and ethical use and sharing of information, including sensitive and classified information as appropriate.	Protect; Detect
Event and Incident Response	Detect Cybersecurity Events	There is a point of contact (person or role) to whom cybersecurity events could be reported.	Detect; Respond
Event and Incident Response	Detect Cybersecurity Events	Detected cybersecurity events are reported.	Detect; Respond
Event and Incident Response	Detect Cybersecurity Events	Cybersecurity events are logged and tracked.	Detect; Respond
Event and Incident Response	Detect Cybersecurity Events	Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events).	Detect; Respond
Event and Incident Response	Detect Cybersecurity Events	There is a repository where cybersecurity events are logged, based on the established criteria.	Detect; Respond
Event and Incident Response	Detect Cybersecurity Events	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features.	Detect; Respond
Event and Incident Response	Detect Cybersecurity Events	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.	Detect; Respond
Event and Incident Response	Detect Cybersecurity Events	The COP for the function is monitored to support the identification of cybersecurity events (SA-3a).	Detect; Respond
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	Criteria for cybersecurity event escalation are established, including cybersecurity incident declaration criteria.	Detect; Respond; Recover
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	Cybersecurity events are analyzed to support escalation and the declaration of cybersecurity incidents.	Detect; Respond; Recover
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	Escalated cybersecurity events and incidents are logged and tracked.	Detect; Respond
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	Criteria for cybersecurity event escalation, including cybersecurity incident criteria, are established, based on the potential impact to the function.	Detect; Respond
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are updated at an organization-defined frequency.	Detect; Respond

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure.	Detect; Respond
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	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).	Detect; Respond
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	Escalated cybersecurity events and declared cybersecurity incidents inform the COP (SA-3a) for the function.	Detect; Respond
Event and Incident Response	Escalate Cybersecurity Events and Declare Incidents	Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident response personnel are identified, and roles are assigned.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Responses to escalated cybersecurity events and incidents are implemented to limit impact to the function and restore normal operations.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, ICS-CERT, relevant ISACs).	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	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, closure).	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident response plans are exercised at an organization-defined frequency.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident response plans address OT and IT assets important to the delivery of the function.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Training is conducted for cybersecurity event and incident response teams.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken.	Respond; Recover
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident responses are coordinated with law enforcement and other government entities as appropriate, including support for evidence collection and preservation.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., tabletop, simulated incidents).	Detect; Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident response activities are coordinated with relevant external entities.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Cybersecurity event and incident response plans are aligned with the function's risk criteria (RM-1c) and threat profile (TVM-1d).	Respond

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Policy and procedures for reporting cybersecurity event and incident information to designated authorities conform with applicable laws, regulations, and contractual agreements.	Respond
Event and Incident Response	Respond to Incidents and Escalated Cybersecurity Events	Restored assets are configured appropriately, and inventory information is updated, following execution of response plans.	Respond; Recover
Event and Incident Response	Plan for Continuity	The activities necessary to sustain minimum operations of the function are identified.	Respond
Event and Incident Response	Plan for Continuity	The sequence of activities necessary to return the function to normal operation is identified.	Respond; Recover
Event and Incident Response	Plan for Continuity	Continuity plans are developed to sustain and restore operation of the function.	Respond; Recover
Event and Incident Response	Plan for Continuity	Business impact analyses inform the development of continuity plans.	Respond; Recover
Event and Incident Response	Plan for Continuity	Recovery time objectives and recovery point objectives for the function are incorporated into continuity plans.	Respond; Recover
Event and Incident Response	Plan for Continuity	Continuity plans are evaluated and exercised.	Recover
Event and Incident Response	Plan for Continuity	Business impact analyses are periodically reviewed and updated.	Recover
Event and Incident Response	Plan for Continuity	Recovery time objectives and recovery point objectives are aligned with the function's risk criteria (RM-1c).	Recover
Event and Incident Response	Plan for Continuity	The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly.	Recover
Event and Incident Response	Plan for Continuity	Continuity plans are periodically reviewed and updated.	Recover
Event and Incident Response	Plan for Continuity	Restored assets are configured appropriately, and inventory information is updated, following execution of continuity plans.	Recover
Event and Incident Response	Management Activities	Documented practices are followed for cybersecurity event and incident response as well as for continuity-of-operations activities.	Recover
Event and Incident Response	Management Activities	Stakeholders for cybersecurity event and incident response as well as continuity-of-operations activities are identified and involved.	Recover
Event and Incident Response	Management Activities	Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response as well as continuity-of-operations activities.	Recover
Event and Incident Response	Management Activities	Standards and/or guidelines have been identified to inform cybersecurity event and incident response as well as continuity-of-operations activities.	Recover
Event and Incident Response	Management Activities	Cybersecurity event and incident response as well as continuity-of-operations activities are guided by documented policies or other organizational directives.	Recover
Event and Incident Response	Management Activities	Cybersecurity event and incident response as well as continuity-of-operations policies include compliance requirements for specified standards and/or guidelines.	Respond; Recover
Event and Incident Response	Management Activities	Cybersecurity event and incident response as well as continuity-of-operations activities are periodically reviewed to ensure conformance with policy.	Respond; Recover
Event and Incident Response	Management Activities	Responsibility and authority for the performance of cybersecurity event and incident response as well as continuity-of-operations activities are assigned to personnel.	Respond
Event and Incident Response	Management Activities	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.	Respond

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Supply Chain Enterprise Data Management (EDM)	Identify Dependencies	Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function depend, including operating partners).	Identify
Supply Chain EDM	Identify Dependencies	Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function, including operating partners).	Identify
Supply Chain EDM	Identify Dependencies	Supplier dependencies are identified according to established criteria.	Identify
Supply Chain EDM	Identify Dependencies	Customer dependencies are identified according to established criteria.	Identify
Supply Chain EDM	Identify Dependencies	Single-source and other essential dependencies are identified.	Identify
Supply Chain EDM	Identify Dependencies	Dependencies are prioritized.	Identify; Protect
Supply Chain EDM	Identify Dependencies	Dependency prioritization and identification are based on the function's or organization's risk criteria (RM-1c).	Identify; Protect
Supply Chain EDM	Manage Dependency Risk	Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed.	Identify
Supply Chain EDM	Manage Dependency Risk	Cybersecurity requirements are considered when establishing relationships with suppliers and other third parties.	Identify
Supply Chain EDM	Manage Dependency Risk	Identified cybersecurity dependency risks are entered into the risk register (RM-2j).	Identify
Supply Chain EDM	Manage Dependency Risk	Contracts and agreements with third parties incorporate sharing of cybersecurity threat information.	Identify
Supply Chain EDM	Manage Dependency Risk	Cybersecurity requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate.	Identify
Supply Chain EDM	Manage Dependency Risk	Agreements with suppliers and other external entities include cybersecurity requirements.	Identify
Supply Chain EDM	Manage Dependency Risk	Evaluation and selection of suppliers and other external entities include consideration of their ability to meet cybersecurity requirements.	Identify
Supply Chain EDM	Manage Dependency Risk	Agreements with suppliers require notification of cybersecurity incidents related to the delivery of the product or service.	Identify
Supply Chain EDM	Manage Dependency Risk	Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements.	Identify; Protect
Supply Chain EDM	Manage Dependency Risk	Cybersecurity risks due to external dependencies are managed according to the organization's risk-management criteria and process.	Identify
Supply Chain EDM	Manage Dependency Risk	Cybersecurity requirements are established for supplier dependencies, based on the organization's risk criteria (RM-1c).	Identify
Supply Chain EDM	Manage Dependency Risk	Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products.	Identify
Supply Chain EDM	Manage Dependency Risk	Acceptance testing of procured assets includes testing for cybersecurity requirements.	Identify
Supply Chain EDM	Manage Dependency Risk	Information sources are monitored to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services).	Identify
Supply Chain EDM	Management Activities	Documented practices are followed for managing dependency risk.	Identify
Supply Chain EDM	Management Activities	Stakeholders for managing dependency risk are identified and involved.	Identify
Supply Chain EDM	Management Activities	Adequate resources (people, funding, and tools) are provided to support dependency risk-management activities.	Identify
Supply Chain EDM	Management Activities	Standards and/or guidelines have been identified to inform managing dependency risk.	Identify

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Supply Chain EDM	Management Activities	Dependency risk-management activities are guided by documented policies or other organizational directives.	Identify
Supply Chain EDM	Management Activities	Dependency risk-management policies include compliance requirements for specified standards and/or guidelines.	Identify
Supply Chain EDM	Management Activities	Dependency risk-management activities are periodically reviewed to ensure conformance with policy.	Identify
Supply Chain EDM	Management Activities	Responsibility and authority for the performance of dependency risk management are assigned to personnel.	Identify
Workforce Management	Assign Cybersecurity Responsibilities	Cybersecurity responsibilities for the function are identified.	Identify
Workforce Management	Assign Cybersecurity Responsibilities	Cybersecurity responsibilities are assigned to specific people.	Identify
Workforce Management	Assign Cybersecurity Responsibilities	Cybersecurity responsibilities are assigned to specific roles, including external service providers.	Identify
Workforce Management	Assign Cybersecurity Responsibilities	Cybersecurity responsibilities are documented (e.g., in position descriptions).	Identify
Workforce Management	Assign Cybersecurity Responsibilities	Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate.	Identify
Workforce Management	Assign Cybersecurity Responsibilities	Cybersecurity responsibilities are included in job performance evaluation criteria.	Identify
Workforce Management	Assign Cybersecurity Responsibilities	Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage.	Identify
Workforce Management	Control the Workforce Life Cycle	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.	Protect
Workforce Management	Control the Workforce Life Cycle	Personnel termination procedures address cybersecurity.	Protect
Workforce Management	Control the Workforce Life Cycle	Personnel vetting is performed at an organization-defined frequency for positions that have access to the assets required for delivery of the function.	Protect
Workforce Management	Control the Workforce Life Cycle	Personnel transfer procedures address cybersecurity.	Protect
Workforce Management	Control the Workforce Life Cycle	Risk designations are assigned to all positions that have access to the assets required for delivery of the function.	Protect
Workforce Management	Control the Workforce Life Cycle	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation.	Protect
Workforce Management	Control the Workforce Life Cycle	Succession planning is performed for personnel based on risk designation.	Protect
Workforce Management	Control the Workforce Life Cycle	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures.	Protect
Workforce Management	Develop Cybersecurity Workforce	Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities.	Protect
Workforce Management	Develop Cybersecurity Workforce	Cybersecurity knowledge, skill, and ability gaps are identified.	Protect
Workforce Management	Develop Cybersecurity Workforce	Identified gaps are addressed through recruiting and/or training.	Identify; Protect
Workforce Management	Develop Cybersecurity Workforce	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).	Protect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Workforce Management	Develop Cybersecurity Workforce	Cybersecurity workforce management objectives that support current and future operational needs are established and maintained.	Protect
Workforce Management	Develop Cybersecurity Workforce	Recruiting and retention are aligned to support cybersecurity workforce management objectives.	Protect
Workforce Management	Develop Cybersecurity Workforce	Training programs are aligned to support cybersecurity workforce management objectives.	Protect
Workforce Management	Develop Cybersecurity Workforce	The effectiveness of training programs is evaluated at an organization-defined frequency, and improvements are made as appropriate.	Protect
Workforce Management	Develop Cybersecurity Workforce	Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities.	Protect
Workforce Management	Increase Cybersecurity Awareness	Cybersecurity awareness activities occur.	Protect
Workforce Management	Increase Cybersecurity Awareness	Objectives for cybersecurity awareness activities are established and maintained.	Protect
Workforce Management	Increase Cybersecurity Awareness	Cybersecurity awareness content is based on the organization's threat profile (TVM-1d).	Protect
Workforce Management	Increase Cybersecurity Awareness	Cybersecurity awareness activities are aligned with the predefined states of operation (SA-3f).	Protect
Workforce Management	Increase Cybersecurity Awareness	The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency, and improvements are made as appropriate.	Protect
Workforce Management	Management Activities	Documented practices are followed for cybersecurity workforce management activities.	Protect
Workforce Management	Management Activities	Stakeholders for cybersecurity workforce management activities are identified and involved.	Protect
Workforce Management	Management Activities	Adequate resources (people, funding, and tools) are provided to support cybersecurity workforce management activities.	Protect
Workforce Management	Management Activities	Standards and/or guidelines have been identified to inform cybersecurity workforce management activities.	Protect
Workforce Management	Management Activities	Cybersecurity workforce management activities are guided by documented policies or other organizational directives.	Protect
Workforce Management	Management Activities	Cybersecurity workforce management policies include compliance requirements for specified standards and/or guidelines.	Protect
Workforce Management	Management Activities	Cybersecurity workforce management activities are periodically reviewed to ensure conformance with policy.	Protect
Workforce Management	Management Activities	Responsibility and authority for the performance of cybersecurity workforce management activities are assigned to personnel.	Protect
Workforce Management	Management Activities	Personnel performing cybersecurity workforce management activities have the skills and knowledge needed to perform their assigned responsibilities.	Protect
Cybersecurity Program Management	Establish Cybersecurity Program Strategy	The cybersecurity program strategy and priorities are documented and aligned with the organization's strategic objectives and risk to critical infrastructure.	Protect
Cybersecurity Program Management	Establish Cybersecurity Program Strategy	The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities.	Protect
Cybersecurity Program Management	Establish Cybersecurity Program Strategy	The cybersecurity program strategy defines the structure and organization of the cybersecurity program.	Identify; Protect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Cybersecurity Program Management	Establish Cybersecurity Program Strategy	The cybersecurity program strategy is approved by senior management.	Protect
Cybersecurity Program Management	Establish Cybersecurity Program Strategy	The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVM-1d).	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	Resources (people, tools, and funding) are provided to support the cybersecurity program.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	Senior management provides sponsorship for the cybersecurity program.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	The cybersecurity program is established according to the cybersecurity program strategy.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	Adequate funding and other resources (i.e., people and tools) are provided to establish and operate a cybersecurity program aligned with the program strategy.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	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).	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	The development and maintenance of cybersecurity policies is sponsored.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	Responsibility for the cybersecurity program is assigned to a role with requisite authority.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	The performance of the cybersecurity program is monitored to ensure it aligns with the cybersecurity program strategy.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	The cybersecurity program is independently reviewed (i.e., by reviewers who are not in the program) for achievement of cybersecurity program objectives.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	The cybersecurity program addresses and enables the achievement of regulatory compliance as appropriate.	Protect
Cybersecurity Program Management	Sponsor Cybersecurity Program	The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives.	Protect
Cybersecurity Program Management	Establish and Maintain Cybersecurity Architecture	A strategy to architecturally isolate the organization's IT systems from OT systems is implemented.	Protect
Cybersecurity Program Management	Establish and Maintain Cybersecurity Architecture	A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy.	Protect
Cybersecurity Program Management	Establish and Maintain Cybersecurity Architecture	Architectural segmentation and isolation are maintained according to a documented plan.	Protect

Domain	Subdomain	ES-C2M2 Objective	NIST CSF
Cybersecurity Program Management	Establish and Maintain Cybersecurity Architecture	Cybersecurity architecture is updated at an organization-defined frequency to keep it current.	Protect
Cybersecurity Program Management	Perform Secure Software Development	Software to be deployed on assets important to the delivery of the function is developed using secure software development practices.	Protect
Cybersecurity Program Management	Perform Secure Software Development	Policies require that software to be deployed on assets important to the delivery of the function be developed using secure software development practices.	Protect
Cybersecurity Program Management	Management Activities	Documented practices are followed for cybersecurity program management activities.	Protect
Cybersecurity Program Management	Management Activities	Stakeholders for cybersecurity program management activities are identified and involved.	Protect
Cybersecurity Program Management	Management Activities	Standards and/or guidelines have been identified to inform cybersecurity program management activities.	Protect
Cybersecurity Program Management	Management Activities	Cybersecurity program management activities are guided by documented policies or other organizational directives.	Protect
Cybersecurity Program Management	Management Activities	Cybersecurity program management activities are periodically reviewed to ensure conformance with policy.	Protect
Cybersecurity Program Management	Management Activities	Personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities.	Protect

A.2 Cyber-Physical Technical Management

The technical portion of the assessment applies to DERs and their surrounding systems only.

Table A.2. Cyber-Physical Technical Management

Domain	Subdomain	Technical Management Objective	NIST CSF
Account Management	Monitoring	There is a site policy that defines a limit to the number of consecutive invalid login attempts by a user.	Protect
Account Management	Monitoring	Remote connections to the distributed energy resource (DER) system are actively monitored, including scanning of unauthorized wireless access points.	Protect
Account Management	Monitoring	The location's facility operations authorize, authenticate, and monitor the use of guest/anonymous accounts to the DER system.	Protect
Account Management	Monitoring	Sensors are included or added to monitor critical status and measurements, such as switch status, component temperature, speed, vibration, flow, pressure, and so on to the DER equipment.	Protect
Account Management	Role-Based Access Control (RBAC)	Administrative access to DER controllers is regulated.	Protect
Account Management	RBAC	Individuals with general access to DER controllers are vetted.	Protect
Account Management	RBAC	The system has security measures in place (e.g., two-factor authentication, password management) to prevent unauthorized access to controllers and smart meters.	Protect
Account Management	RBAC	Read-and-write access is given only as appropriate to the facilities' DER management system.	Protect
Account Management	RBAC	The DER system includes predefined roles for the DER owner, DER operator, aggregator, and utility operations manager, at a minimum.	Identify
Account Management	RBAC	Read/write privileges for PPA and/or energy leases on the DER system take remote access security precautions.	Protect
Account Management	Remote access	Remote sessions (if applicable) by companies that provide power purchase agreements (PPAs) and energy leases are monitored.	Protect
Account Management	Remote access	The location has components from the ICS/DER environment that interconnect.	Protect
Account Management	Remote access	There is a policy that mandates a lockout cycle for remote access. The system limits the number of remote connections that can be active at any given time.	Protect
Account Management	Remote Access	The energy management system restricts the number of access points.	Protect
Account Management	Logging	Sensors on the system monitor critical status and measurements, such as switch status, component temperature, speed, vibration, flow, pressure, and so on.	Detect
Account Management	Logging	The DER system validates even authorized changes to DER operational settings, based on what those settings are reasonably or contractually allowed to be.	Protect
Account Management	Logging	The system rejects any compromised or invalid data.	Protect
Account Management	Logging	Logs are significant to events, data values and status of related equipment. Logs are timestamped.	Protect
Account Management	Logging	Forensic assessment tools are used to extract potential problems with the logging system.	Detect
Account Management	Logging	Post-event engineering forensic analysis capabilities include the security-related actions of DER systems.	Respond
Account Management	Logging	The DER logs when external devices are plugged in.	Protect; Detect

Domain	Subdomain	Technical Management Objective	NIST CSF
Account Management	Authentication, Authorization, and Accounting (AAA)	The location manages authorization of DER information system accounts.	Protect
Account Management	AAA	The location enforces separation of DER information system functions (in terms of privileges) that require access authorization.	Protect
Account Management	AAA	The DER system limits security function to the fewest users necessary.	Protect
Account Management	AAA	The location manages activation of DER system accounts.	Protect
Account Management	AAA	The DER system prohibits data to be provided to unauthenticated users.	Protect
Account Management	AAA	The DER system automatically audits account creation, modification, disabling, and termination actions.	Protect
Configuration	Access control	The location has developed, implemented, reviewed, and updated the access control security policies.	Protect
Configuration	Access control	The location has defined, documented, and approved individual access privileges and enforced access controls associated with configuration changes to the DER system.	Protect
Configuration	Cloud Management	The DER system disables cloud storage by default.	Protect
Configuration	Settings	The location has a controlled, audited, and manual override of automated mechanisms in the event of emergencies.	Protect; Detect
Configuration	Settings	The system performs input validation (i.e., limits and boundaries, formatting, and timing constraints).	Protect
Configuration	Settings	Data received from sensors is authenticated.	Protect
Configuration	Settings	The DER prohibits the connection of external media (e.g., USB, CD.).	Protect
Configuration	Settings	Firewall rules are in place to mitigate denial-of-service attacks.	Protect
Configuration	Change Management	The location has established terms and conditions for installing new hardware, firmware, or software on DER devices.	Identify
Configuration	Change Management	The location conducts security audits of DER system changes at a self-defined frequency.	Identify
Configuration	Software Integrity	The DER system is hardened such that only essential software and applications are installed.	Protect
System/Device management	Software Integrity	The DER system provides an application whitelist.	Identify; Protect
System/Device management	Software Integrity	The DER system uses penetration testing, fuzzing, and other security testing techniques to ensure a hardened system.	Protect
System/Device management	Software Integrity	The DER system contains secure firmware or hardware modules for cryptographic processes of passwords and other embedded private and/or confidential data.	Protect
System/Device management	Software Integrity	The DER system segregates access to sensitive data, depending on the source of the request.	Protect
System/Device management	Software Integrity	The DER system has mechanisms in place to ensure that hardware and firmware (both in-house and purchased) cannot be damaged by faulty software.	Protect
System/Device management	Protection	The system has measures for preventing malware injection.	Protect; Detect
System/Device management	Protection	Internal campaigns for phishing attempts are run regularly and provide training against social engineering attacks.	Protect

Domain	Subdomain	Technical Management Objective	NIST CSF
System/Device management	Protection	There are restrictions on the number of propriety protocols implemented.	Protect
System/Device management	Protection	The energy management system restricts the number of access points.	Protect
System/Device management	Protection	There are enforced policies on healthy password management and use.	Protect
System/Device management	Protection	The environment has a signature or behavioral-based intrusion detection and/or prevention system.	Protect
System/Device management	Patch Management	There is a document policy that records and enforces patch management for operating systems, firmware, and network services.	Identify
System/Device management	Fail-safe	The DER system components use a heartbeat feature to detect potential failure.	Protect
System/Device management	Fail-safe	The DER system provides an emergency manual override that shuts down the entire system.	Respond
System/Device management	Cryptography	Key exchange and trusted computing operations are in place for DER communications.	Protect
System/Device management	Cryptography	Information pertaining to available energy is properly secured at rest and is not shared.	Protect
System/Device management	Cryptography	Full-disk encryption is implemented for data at rest and data in transit.	Protect
System/Device management	Cryptography	Transport layer security (TLS) 1.2. or 1.3 is used wherever applicable.	Protect
System/Device management	Cryptography	The system supports message authentication codes wherever applicable.	Protect
System/Device management	Certificates	The system's DER controls support the use of certificate authorities and the use of multiple certificate authorities.	Protect
System/Device management	Certificates	The DER system implements a certification revocation list.	Protect

A.3 Physical Security

The physical security portion of the assessment applies to the DER system and the organization as a whole.

Table A.3. Physical Security

Domain	Subdomain	Physical Security Objective	NIST CSF
Administrative	Auditing	There are physical access authorization agreements assigned to DER assets.	Protect
Administrative	Auditing	Third-party-provided physical security solutions comply with current standards and requirements, from procurement through implementation and maintenance.	Protect
Administrative	Auditing	Individuals responsible for DER physical security are associated with the primary functional group that is in charge of the site's physical security.	Identify
Administrative	Auditing	Physical security assets and controls are deployed in accordance with applicable federal laws, executive orders, regulations, policies, and standards.	Protect
Administrative	Auditing	The effectiveness of physical security controls at alternate work sites is assessed, as feasible.	Identify
Administrative	Auditing	Physical security controls implemented at the main site are the same for alternate work sites.	Protect
Administrative	Auditing	Physical access audit logs are maintained for entry/ exit points to areas where DER system equipment is housed.	Identify
Administrative	Holistic Security & Contingency Planning	Physical security controls and related processes are managed by a central monitoring station.	Identify
Administrative	Holistic Security & Contingency Planning	Changes to the DER physical security architecture are reflected in the security plan, the security concept of operations (CONOPS), and/or organizational procurements/acquisition processes.	Identify
Administrative	Holistic Security & Contingency Planning	The physical security architecture is updated at a specified frequency to reflect updates in the enterprise architecture.	Identify
Administrative	Holistic Security & Contingency Planning	The physical security architecture for the DER system takes into consideration any security assumptions about, and dependencies on, external services.	Identify
Administrative	Holistic Security & Contingency Planning	The CONOPS is reviewed and updated at a specific frequency or on an incident basis.	Identify
Administrative	Holistic Security & Contingency Planning	The CONOPS for the DER information system incorporates physical security considerations.	Identify
Administrative	Holistic Security & Contingency Planning	The physical security plan is reviewed for the DER system, as it relates to the site security plan at a specific frequency or on an incident basis.	Identify
Administrative	Holistic Security & Contingency Planning	Copies of the physical security plan are distributed to identified key personnel.	Identify
Administrative	Holistic Security & Contingency Planning	All subsequent changes to the physical security plan are communicated to the appropriate key personnel.	Identify
Administrative	Holistic Security & Contingency Planning	The physical security plan for the DER system is reviewed and approved by an authorizing official or designated representative prior to implementation.	Identify

Domain	Subdomain	Physical Security Objective	NIST CSF
Administrative	Holistic Security & Contingency Planning	The physical security plan for the DER system identifies any relevant overlaps, if applicable.	Identify
Administrative	Holistic Security & Contingency Planning	The physical security plan for the DER system includes explicit definitions of the authorization boundary for the system.	Identify
Administrative	Holistic Security & Contingency Planning	The physical security plan for the DER system is consistent with the enterprise physical security architecture.	Identify
Administrative	Holistic Security & Contingency Planning	DER system output devices are marked or labeled, indicating the appropriate physical security level of the personnel allowed to have physical access.	Protect
Administrative	Holistic Security & Contingency Planning	The current physical security planning policies and procedures are reviewed and updated at a specific frequency.	Identify
Administrative	Holistic Security & Contingency Planning	There is a developed, documented and readily available physical protection policy that addresses the purpose, scope, roles, and responsibilities of physical security personnel.	Identify
Administrative	Holistic Security & Contingency Planning	There is a procedural system instated to ensure policies, plans, and procedures for physical security controls are not disclosed to unauthorized personnel, outside of a need to know structure.	Protect
Administrative	Personnel Security Planning	Risk designations are assigned to all organizational positions that operate the DER system in any function.	Protect
Administrative	Personnel Security Planning	The list of individuals with authorized physical access to the facility is developed, approved, and maintained where the DER system resides.	Protect
Administrative	Personnel Security Planning	Individuals are screened prior to being authorized physical access to the DER system.	Protect
Administrative	Personnel Security Planning	Physical access authorization is modified as needed to correspond with any changes in operational need, due to reassignment or transfer.	Protect
Administrative	Personnel Security Planning	Authorization credentials are issued for all facility areas with access to DER systems.	Protect
Administrative	Personnel Security Planning	Individuals are reevaluated to confirm ongoing operational need for authorization to access DER systems.	Protect
Administrative	Personnel Security Planning	Individuals are removed from the facility access list when access is no longer valid or required.	Protect
Administrative	Personnel Security Planning	DER system credentials for terminated individuals are strategically revoked.	Protect
Administrative	Personnel Security Planning	Physical security personnel are notified within a specific time period when an individual's physical access is granted or revoked.	Detect
Administrative	Personnel Security Planning	Exit interviews are conducted that include a discussion of DER physical security topics.	Protect
Administrative	Personnel Security Planning	There is a formal sanctions process that is enforced for individuals failing to comply with established physical security policies and procedures.	Protect
Administrative	Personnel Security Planning	Personnel security requirements are established and enforced, including physical security roles and responsibilities for third-party providers.	Protect
Administrative	Personnel Security Planning	Third-party providers and contractors return organizational badges and equipment upon termination.	Protect
Administrative	Personnel Security Planning	Rules of behavior are developed for the main facility and any remote locations.	Protect

Domain	Subdomain	Physical Security Objective	NIST CSF
Administrative	Personnel Security Planning	The rules of behavior are reviewed and updated for the main facility and any relevant remote locations.	Protect
Administrative	Personnel Security Planning	All authorized individuals with access to the DER system are trained in safety procedures related to the site.	Protect
Administrative	Personnel Security Planning	Visitor access records are maintained to the facility where the DER system resides.	Detect
Administrative	Personnel Security Planning	Visitors are physically escorted and monitored under specific circumstances.	Protect
Administrative	Personnel Security Planning	The visitor access list, detailing authorized facility physical access for defined external individuals, is periodically reviewed.	Detect
Administrative	Personnel Security Planning	Visitor access records are reviewed and verified at a specified frequency.	Detect
Assets	Equipment	There is an alternate power supply provided for the DER system equipment that is not reliant on external power generation.	Respond
Assets	Equipment	There is a capability to automatically switch to the main grid supply in the event of DER system failure for services reliant on the site's DER.	Respond
Assets	Equipment	There is a capability to manually shut off power to the DER system equipment or individual system components in emergency situations.	Respond
Assets	Equipment	Emergency power shutoff capabilities are protected from physically accessed unauthorized activation.	Protect
Assets	Equipment	Power equipment and power cabling for the DER system equipment is protected from damage or destruction in any way.	Protect
Assets	Equipment	There is an emergency communication method from within the DER system control room for emergencies.	Respond
Assets	Equipment	There is automatic emergency lighting deployed and maintained around the DER system equipment, which activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Respond
Assets	Maintenance	The information surrounding the location to keys, combinations, and other physical access devices is secured from unauthorized personnel.	Protect
Assets	Maintenance	There is a master key leveling system in place to ensure physical keys assigned to different personnel don't give them access to unauthorized areas.	Protect
Assets	Maintenance	Combinations and keys are changed when keys are lost, combinations are compromised, or individuals that had access to relevant locks are transferred or terminated.	Respond
Assets	Maintenance	Critical physical security access devices are inventoried at a defined frequency.	Identify; Detect
Assets	Maintenance	There are mechanisms to protect the DER system from damage, as a result from water leakage, by providing a master shutoff or isolation valves that are accessible, working properly, and known to defined key personnel.	Respond
Assets	Maintenance	Fire suppression and detection devices/systems are employed and maintained for the DER system equipment and are supported by an independent energy source.	Respond
Assets	Maintenance	Asset location technologies are deployed to track and monitor the location and movement of critical assets that cannot be misplaced within controlled areas.	Protect
Assets	Maintenance	Temperature and humidity levels within the facility where the DER information system resides are maintained at defined, acceptable levels.	Detect
Assets	Maintenance	Temperature and humidity levels are monitored, with respect to the DER system, at a defined frequency.	Detect

Domain	Subdomain	Physical Security Objective	NIST CSF
Structure	Distancing Practices for Sensitive Assets	DER system components are positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized physical access, which would occur if positioned anywhere else.	Protect
Structure	Distancing Practices for Sensitive Assets	Through strategic location placement, DER system equipment is protected from information leakage and damage, as well as from electromagnetic signals emanations/pulses.	Protect
Structure	Intrusion Detection and Prevention	Physical access to the DER system equipment's distribution and transmission lines is monitored with reasonable security safeguards.	Detect
Structure	Intrusion Detection and Prevention	There are specific security safeguards to monitor and prevent unauthorized access to areas within the facility where the general public has access.	Detect
Structure	Intrusion Detection and Prevention	There are tamper protection controls for DER system equipment, system components, and/or DER facility physical access systems.	Protect
Structure	Response Teams & Force Protection	There is a dedicated protective force personnel on the facility site where DER systems reside.	Respond; Recover
Structure	Response Teams & Force Protection	Clearly defined roles and responsibilities are outlined and defined for the protective force personnel within a structured organization.	Protect
Structure	Response Teams & Force Protection	Standard operating procedures are implemented for the appropriate response teams to follow when physical security incidents at facilities occur.	Respond; Recover
Structure	Response Teams & Force Protection	Physical access authorization is enforced at defined entry/exit points to the facility, using electronic access controls and/or guards.	Protect
Structure	Response Teams & Force Protection	There are protective force partnerships and interoperability plans with surrounding response agencies in the event that a physical security incident were to escalate beyond their the primary protective force's capacity and capabilities.	Respond; Recover