Cybersecurity Baselines for Electric Distribution Utilities and DER

DRAFT INFORMATIVE REFERENCES

February 2024

This is a companion document to the
Cybersecurity Baselines for Electric Distribution Utilities and DER

DRAFT Informative References

The Cybersecurity Baselines represent widely applicable cybersecurity practices that are drawn from and aligned with common cybersecurity risk management frameworks, standards, and guidelines used in the energy sector. The Steering Committee has identified several of these resources and conducted a cursory review to identify specific practices or elements that are related to each of the recommended Cybersecurity Baselines. The informative references are intended to be illustrative and are not exhaustive. These references may serve as additional guidance for interpreting the baselines.

This analysis will be heavily reviewed and revised in Phase 2 for accuracy, relevancy, and completeness.

Cautions on Using the Informative References

Users must recognize the following considerations and limitations when reviewing the resources referenced in the table:

- The identified practices under each informative reference **do not represent equivalent or interchangeable practices** for the corresponding Cybersecurity Baseline.
- Referenced practices **do not provide a means to implement or demonstrate achievement** of the Cybersecurity Baselines. Implementation of a referenced practice does not indicate or imply that an organization has implemented the Cybersecurity Baseline.
- The analysis represents only a cursory review of potential alignment between the Cybersecurity Baseline and other informative resources. **Additional review is needed to ensure accuracy or relevancy**.
- **Referenced practices are relevant only to the corresponding Cybersecurity Baseline**. References have not been considered for relevancy to each other, and users should not interpret that referenced practices from different resources have been mapped to each other in any way. Users **should not consult this analysis to inform implementation of any of the referenced standards**, particularly regulatory standards.

Types of Informative References

The referenced practices may provide example practices, processes, requirements, and documentation to inform adoption of the Cybersecurity Baselines. Referenced resources include:

- **Voluntary cybersecurity frameworks and guidelines for critical infrastructure**—Commonly used frameworks that support energy infrastructure owners and operators in making risk-based cybersecurity decisions.
- **Voluntary standards for system implementation or manufacturing**—Common standards for device or system manufacturing, integration, and/or implementation that may serve as additional guidance for interpreting the Cybersecurity Baselines.
- **Regulatory standards applicable to select energy companies**—While these regulations apply to assets outside of the scope of the Distribution and DER Cybersecurity Baselines, energy companies may wish to leverage lessons learned or existing management processes within their organizations when implementing the Cybersecurity Baselines.

Summary of References

The Informative References table references the following resources:

Voluntary Cybersecurity Frameworks and Guidelines

U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)

Cross-Sector Cybersecurity Performance Goals (CPGs), Version 1.0.1

March 2023 | cisa.gov/cross-sector-cybersecurity-performance-goals

Voluntary | Applicable to: all critical infrastructure organizations in any sector

Voluntary cybersecurity practices for all critical infrastructure organizations that are intended to provide a baseline of cybersecurity practices that all entities can implement to reduce known risks. As baseline practices, they are intended to help small- and medium-sized organizations kickstart their cybersecurity efforts. CISA is working with individual sectors to tailor the CPGs for sector-specific applicability. *Note:* The "Other IR" column in the table includes additional references that CISA identified as relevant to the CPGs.

National Institute of Standards and Technology (NIST)

Cybersecurity Framework (CSF) Version 1.1

April 2018 | nist.gov/cyberframework

Voluntary | Applicable to: critical infrastructure asset owners and operators in any sector

Voluntary cyber risk management framework for use by critical infrastructure asset owners and operators in any sector. It references recognized standards and guidelines, and offers a framework to build or improve a cybersecurity program organized around five key Functions: Identify, Protect, Detect, Respond, and Recover.

U.S. Department of Energy

Cybersecurity Capability Maturity Model (C2M2), Version 2.1

June 2022 | energy.gov/C2M2

Voluntary | Applicable to: asset owners and operators in the energy sector and any critical infrastructure sector

Voluntary, free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both IT and OT assets and environments. Organizations can use the C2M2 to consistently measure their cybersecurity capabilities over time, identify target maturity levels based on risk, and prioritize the actions and investments that allow them to meet their targets.

Voluntary Standards for System Implementation or Manufacturing

National Institute of Standards and Technology (NIST)

SP 800-53 Rev. 4/5: Security and Privacy Controls for Information Systems and Organizations

September 2020 | csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Voluntary | Applicable to: federal information systems and information systems or organizations in any sector

Provides a catalog of security and privacy controls for information systems and organizations to protect from diverse risks. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk.

Important note: Some items reference Rev. 4; an additional review will need to be done in Phase 2 to update the references.

International Society of Automation (ISA) and International Electrotechnical Commission (IEC)

ISA/IEC 62443 Series of Standards: Security for Industrial Automation and Control Systems

isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Voluntary | Applicable to: any industry sector that uses industrial automation and control

Global series of standards that define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems. These standards set best practices for security and provide a way to assess the level of security performance. With use cases from more than 20 different industries, the ISA/IEC 62443 series of standards have demonstrated their utility in all industry verticals that use OT. Work is ongoing to further develop application profiles for the energy sector.

International Organization for Standardization (ISO) and IEC

ISO/IEC 27001:2013: Information Security, Cybersecurity, and Privacy Protection

2013| iso.org/standard/27001

Voluntary | Applicable to: information security management systems in any sector

Standard that defines the requirements that information security management systems must meet, providing companies with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Important note: The table refers to a version of the standard that has been superseded by a 2022 update; an additional review will need to be done in Phase 2 to update the references.

IEEE Standards Association

IEEE 1547.3-2023: Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

March 5, 2020 | standards.ieee.org/ieee/1547.3/10173/

Voluntary | Applicable to: DER manufacturers, operators, and system integrators

Guidelines for cybersecurity of DER interconnection with electric power systems.

Important note: The table references selected IEEE 1547.3 cybersecurity requirements derived from the IEEE 1547.3 recommendations, as identified by the CPUC Smart Inverter Operationalization Cybersecurity (SIO-CS) Subgroup.

SunSpec Alliance

DER Cybersecurity Specifications – Phase 1 Requirements

sunspec.org/specifications/

Voluntary | Applicable to: DER manufacturers

The SunSpec Alliance is an open information standards and certification organization for distributed energy resources (DER). SunSpec provides DER interoperability, data communications and cybersecurity functionality standards, aligned with international and national protocols, and provides a testing and certification program that approves devices which meet those standards. Cybersecurity Baselines were reviewed against the DER Cybersecurity Specifications.

Regulatory Standards for Select Energy Systems

North American Electric Reliability Corporation (NERC)

Critical Infrastructure Protection (CIP) Cyber Security Standards

Individual revision dates | nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

Mandatory | Applicable to: entities operating within the North American bulk electric system (BES) with assets that meet size and criticality criteria

Mandatory cybersecurity standards for entities operating within the North American bulk electric system (BES) and applicable to assets that meet size and criticality criteria. Reliability standards for cybersecurity consist of CIP-002 to CIP-013 and are mandated and enforced by the Federal Energy Regulatory Commission (FERC). Note: The Distribution and DER baselines are primarily designed for assets that do not meet the applicability criteria for NERC CIP standards; however, entities may leverage best practices or compliance frameworks.

U.S. Department of Homeland Security (DHS) Transportation Security Administration (TSA)

Security Directive Pipeline-2021-02D

July 27, 2023 | tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf

Mandatory | Applicable to: TSA-specified owners and operators of critical pipeline and liquefied natural gas facilities

Performance-based regulatory cybersecurity measures that are applicable to TSA-specified owners and operators of critical pipeline and liquefied natural gas facilities.

Future References to Consider

The Steering Committee plans to examine other informative references relevant to the Cybersecurity Baselines in Phase 2. One of the references that will be considered is the UL Solutions draft standard UL 2941: Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources. This voluntary standard aims to provide testable requirements for DERs, but is too early in development to include at this time.

DRAFT Informative References for the Cybersecurity Baselines for Electric Distribution Utilities and DER

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
1.A Asset Inventory	Maintain an inventory of critical IT and digital OT assets, using the organization's risk-based criteria for classifying the criticality of assets that are essential to the delivery of energy.	**1.A Asset Inventory** Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.	ID.AM-1	THREAT-1a THREAT-1b THREAT-1d THREAT-1e THREAT-1g THREAT-3a ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h	NIST SP 800-53: CM-8	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2	SM-1a, SM-2a	DER/SWUP/REQ-02	CIP-002-5.1a-R1 CIP-002-5.1a-R2	
1.B Organizational Cybersecurity Leadership + 1.C OT Cybersecurity Leadership + 1.D Improving IT and OT Cybersecurity Relationships	Designate a senior-level role/title/position with explicit accountability for governance, planning, resourcing, and executing IT and OT cybersecurity activities. Identify the senior-level role(s)/title(s)/position(s) with delegated responsibility for planning, allocating resources, managing, and executing cybersecurity activities while promoting a culture of cybersecurity.	**1.B Organizational Cybersecurity Leadership** A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning. **1.C OT Cybersecurity Leadership** A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations, this may be the same position as identified in 1.B. **1.D Improving IT and OT Cybersecurity Relationships** Organizations sponsor at least one "pizza party" or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).	ID.GV-1 ID.GV-2	WORKFORCE-1e WORKFORCE-1g WORKFORCE-2a WORKFORCE-2d PROGRAM-2a PROGRAM-2c PROGRAM-2d PROGRAM-2e PROGRAM-2f	NIST SP 800-53: PM-2, PM-29 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM9, PM-10, PM-11	ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.3.3, 4.3.2.4.3, 4.3.2.6, 4.3.2.6.3	ISO/IEC 27001:2013 A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1 Clause 6	RA-19, RA-13, RA-14, RA-15, RA-16, RA-19		CIP-003-8-R3 CIP-003-8-R4 CIP-004-6-R2	
1.E Mitigating Known Vulnerabilities	Establish and implement a vulnerability management plan to address known exploited vulnerabilities, prioritizing critical assets identified in 1.A. Identify compensating controls for critical assets where removing the vulnerability is either	**1.E Mitigating Known Vulnerabilities** All known exploited vulnerabilities (listed in CISA's Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first.	ID.RA-1, PR.IP-12, DE.CM-8, RS.MI-3, ID.RA-6,	THREAT-1a THREAT-1b THREAT-1d THREAT-1e THREAT-1g THREAT-3a ARCHITECTURE-3a	NIST SP 800-53: RA-5, SI-2	ISA 62443-2-1:2009 4.2.3, 4.2.3.1, 4.2.3.7, 4.2.3.9, 4.2.3.12	ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3	RA-3		CIP-007-6-R2 CIP-010-4-R3 CIP-010-4-R4 CIP-007-6-R2 CIP-013-2-R1	III E 1 III E 2 a III E 2 b III E 3

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
	not possible or may substantially compromise availability or safety.	• OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.	RS.AN-5	ARCHITECTURE-3b ARCHITECTURE-3h							
1.F Third-Party Validation of Cybersecurity Control Effectiveness	Develop and implement a plan for periodic independent validation of the organization's cybersecurity controls and mitigate findings in a timely, risk-informed manner.	**1.F Third-Party Validation of Cybersecurity Control Effectiveness** Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. • Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. • High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.	ID.RA-1, ID.RA-3	THREAT-1c THREAT-1d THREAT-1f THREAT-1g THREAT-1k THREAT-3a PROGRAM-2g PROGRAM-2h	NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-12, PM-16	ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12	ISO/IEC 27001:2013 A.12.6.1, A.18.2.3	RA-12		CIP-007-6-R4 CIP-014-3 R4	
1.G Supply Chain Incident Reporting + 1.H Supply Chain Vulnerability Disclosure	As new procurements are made for critical devices or services, make a good faith effort to negotiate procurement documents and contracts to stipulate that vendors and/or service providers: 1. Notify the procuring customer of security incidents within a risk-informed time frame, as determined by the organization. 2. Notify the procuring customer of confirmed security vulnerabilities in	**1.G Supply Chain Incident Reporting** Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization. **1.H Supply Chain Vulnerability Disclosure** Procurement documents and contracts, such as SLAs, stipulate that **vendors and/or service providers notify the procuring customer of confirmed security**	ID.SC-1, ID.SC-3	THIRD-PARTIES-2c THIRD-PARTIES-2f	NIST SP 800-53: SA-9, SR-8	ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7, 4.3.4.2	ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 ISO/IEC 29147 ISO/IEC 30111	SM-11, SM-13		CIP-013-2-R1 CIP-014-3 R6 CIP-013-2-R1 CIP-014-3 R6	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
	their assets within a risk-informed time frame, as determined by the organization.	**vulnerabilities in their assets** within a risk-informed time frame as determined by the organization.									
1.I Vendor/ Supplier Cybersecurity Requirements	Include cybersecurity requirements and questions, as appropriate, in the organization's procurement process, and evaluate responses as part of the overall vendor selection.	**1.I Vendor/ Supplier Cybersecurity Requirements** Organizations' **procurement documents include cybersecurity requirements and questions**, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.	ID.SC-3	THIRD-PARTIES-2a THIRD-PARTIES-2b THIRD-PARTIES-2c THIRD-PARTIES-2d	NIST SP 800-53: SA-9, SR-5, SR-6	ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7	ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3	SM-11, SM-13, SM-14, SM-15		CIP-013-2-R2	
2.A Changing Default Passwords	Establish and maintain a process to change default passwords before installation. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.	**2.A Changing Default Passwords** An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for OT, such as OT administration web pages. • In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices. • OT: While changing default passwords on an organization's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change.	PR.AC-1	ASSET-3a ASSET-3b ASSET-3c ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3e ARCHITECTURE-3h	NIST SP 800-53: IA-5	ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9		NE-37a	DER/AUTH/REQ-06	CIP-003-8-R2	
2.B Password Management	Establish and enforce a policy that requires a minimum password length of 15 or more characters for in-scope IT and OT assets that are not otherwise protected behind an MFA or other passwordless authentication mechanism. • If 15-character passwords, MFA, or other passwordless authentication	**2.B Minimum Password Strength** Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets and all OT assets, when technically feasible.** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not	PR.AC-1	ACCESS-1d ACCESS-4c ARCHITECTURE-1d ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h	NIST SP 800-53: IA-5	ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 XKCD 936		AC-5a	DER/AUTH/REQ-05	CIP-004-6-R5	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
	mechanisms are not feasible, use the maximum password length that the technology supports and document and implement equally or more effective alternative measures or compensating controls to achieve the intended action(s). • Establish a corporate policy to avoid password reuse. Prohibit password reuse unless an organization-defined risk exception is necessary and documented.	technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement. • This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods. • * Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember. • ** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as those on offshore rigs or wind turbines.									
2.C Unique Credentials	Provide unique and separate credentials for users accessing services and assets on IT and OT networks. Establish and implement a process to manage and approve access to shared accounts / service accounts/ machine accounts. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.	**2.C Unique Credentials** Organizations provision unique and separate credentials for similar services and asset access on IT and OT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have passwords that are unique from all member user accounts.	PR.AC-1	ACCESS-1a ACCESS-1b ACCESS-1d ACCESS-2c ACCESS-2f ACCESS-2g ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h	NIST SP 800-53: AC-2, AC-3	ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9		AC-1a	DER/AUTH/REQ-01	CIP-004-7-R4	
2.D Revoking Credentials for Departing Employees	Establish and enforce an administrative process to (1) revoke physical access and (2) disable logical access to critical organizational resources within 24 hours of an employee's exit, unless an organization-	**2.D Revoking Credentials for Departing Employees** A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2)	PR.AC-1	ACCESS-1c ACCESS-1f ACCESS-2b ACCESS-3b ACCESS-4a WORKFORCE-1b WORKFORCE-1d	NIST SP 800-53: AC-2, AC-3	ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5,		AC-17a	DER/AUTH/REQ-09	CIP-007-6-R5	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
	defined risk exception is necessary and documented.	disables all user accounts and access to organizational resources.		WORKFORCE-5a ARCHITECTURE-1d		SR 1.7, SR 1.8, SR 1.9					
2.E Separating User and Privileged Accounts	Establish and maintain a policy to restrict administrator rights on user accounts on critical assets. Require separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Reevaluate privileges on a recurring basis to validate continued need for a given set of permissions. • Document and implement alternative measures or compensating controls in instances where administrative privileges cannot be removed.	**2.E Separating User and Privileged Accounts** No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.	PR.AC-4	ACCESS-1e ACCESS-1g ACCESS-2d ACCESS-2h ACCESS-4c WORKFORCE-1e ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h	NIST SP 800-53: AC-6	ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1		AC-20a		CIP-004-6-R4	
2.F Network Segmentation	Separate IT and OT networks, and OT networks of different trust levels. • Use an appropriate network security device to enforce a deny-by-default policy on communications between networks that permits only those connections that are explicitly allowed (e.g., by IP address and port) for specific system functionality. • Maintain documentation of allowed ports and services and their business justification.	**2.F Network Segmentation** All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.	PR.AC-5, PR.PT-4, DE.CM-1	ASSET-3a ASSET-3b ASSET-3c ARCHITECTURE-1c ARCHITECTURE-2a ARCHITECTURE-2b ARCHITECTURE-2c ARCHITECTURE-2d ARCHITECTURE-2e ARCHITECTURE-2f	NIST SP 800-53: AC-4, SC-7, SI-4	ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 6.2, SR 7.1, SR 7.6	ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	NE-4a		CIP-005-7-R1 CIP-005-7-R3	III B 1
2.G Unsuccessful (Automated) Login Attempts	Implement a process to detect, alert, and monitor unsuccessful logins and to inform the appropriate teams. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.	**2.G Detection of Unsuccessful (Automated) Login Attempts** All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis.	PR.AC-7	ACCESS-2i SITUATION-1a SITUATION-1b SITUATION-1c SITUATION-2a SITUATION-2b SITUATION-2c SITUATION-2e ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h	NIST SP 800-53: AC-7	ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-		AC-7a	DER/AUTH/REQ-07	CIP-005-7-R1	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
		• For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10-minutes after 10 incorrect logins over a 10-minute period.				3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10					
2.H Phishing-Resistant Multifactor Authentication (MFA)	Implement MFA for remote access to assets outside of the control network using the strongest available method for that asset and where technically feasible. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.	**2.H Phishing-Resistant Multifactor Authentication (MFA)** • Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope). MFA options sorted by strength, high to low, are as follows: ○ Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or public key infrastructure (PKI) based - see CISA guidance in ”Resources”); ○ If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used; ○ MFA via short message service (SMS) or voice only used when no other options are possible. • IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems. • OT: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible HMIs.	PR.AC-7	ACCESS-1b ACCESS-1h ACCESS-1i ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h	NIST SP 800-53: IA-2, IA-3	ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10		AC-10		CIP-005-7-R2	III C 2
2.I Basic Cybersecurity Training	Conduct training, at least annually, for all organizational employees and contractors that cover basic security concepts, such as	**2.I Basic Cybersecurity Training** At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as	PR.AT-1	THIRD-PARTIES-2c WORKFORCE-2a WORKFORCE-2b	NIST SP 800-53: AT-2	ISA 62443-2-1:2009 4.3.2.4.2	ISO/IEC 27001:2013 A.7.2.2, A.12.2.1			CIP-003-8-R2 CIP-004-6-R1	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
	phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness. • New employees receive initial cybersecurity training within 30 days of onboarding and recurring training on at least an annual basis. • Training topics and goals are clearly defined and related to the nature of their duties to the extent practical.	phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness. • New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.		WORKFORCE-2c WORKFORCE-2d							
2.J OT Cybersecurity Training	In addition to basic cybersecurity training, conduct OT-specific cybersecurity training, at least annually, for personnel who access or secure OT as part of their regular duties.	**2.J OT Cybersecurity Training** In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.	PR.AT-2, PR.AT-3, PR.AT-5	WORKFORCE-4a WORKFORCE-4d	NIST SP 800-53: AT-3	ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3	ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2			CIP-004-6-R1 CIP-004-7-R1 CIP-013-2-R1	
2.K Strong and Agile Encryption	Establish and implement a policy that addresses the protection of critical data in transit, including how the organization will update outdated/deprecated encryption technologies or document and implement equally or more effective alternative methods or compensating controls.	**2.K Strong and Agile Encryption** Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithms, and consider managing implications of post-quantum cryptography. • OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.	PR.DS-1, PR.DS-2	ARCHITECTURE-1f ARCHITECTURE-1g ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h ARCHITECTURE-5c ARCHITECTURE-5d ARCHITECTURE-6c	NIST SP 800-53: SC-8, SC-13, SC-28	ISA 62443-3-3:2013 SR 3.1, SR 3.4, SR 3.8, SR 4.1, SR 4.2	ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	DS-2a	DER/DCOM/REQ-02	CIP-005-7-R2 CIP-011-2-R1 CIP-012-1-R1 CIP-011-2-R1 CIP-011-3-R1	
2.L Secure Sensitive Data	Establish and maintain a process to identify and securely store sensitive data, using strong access control methods for authenticated and authorized users and system applications. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.	**2.L Secure Sensitive Data** Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.	PR.DS-1, PR.DS-2, PR.DS-5	ASSET-2a ASSET-2b ASSET-2c ASSET-2d ACCESS-2a ACCESS-2c ACCESS-2g ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h ARCHITECTURE-5a	NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, MP-12, PE-19, PS-3, PS-6, SC-7, SC-8, SC-11, SC-12, SC-13, SC-28, SC-31, SI-4	ISA 62443-3-3:2013 SR 3.4, SR 4.1, SR 5.2	ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1,			CIP-005-7-R1 CIP-005-7-R2 CIP-011-2-R1 CIP-012-1-R1 CIP-011-2-R1 CIP-011-3-R1	IV B

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
				ARCHITECTURE-5b ARCHITECTURE-5d			A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3				
2.M Email Security	Establish and maintain a process to reduce risk from email threats.	**2.M Email Security** On all corporate email infrastructure (1) STARTTLS is enabled, (2) Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are enabled, and (3) Domain-based Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies.	PR.DS-1, PR.DS-2, PR.DS-5	WORKFORCE-2a ARCHITECTURE-2a ARCHITECTURE-2g	NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, CM-8, MP-6, MP-8, PE-16, PE-19, PS-3, PS-6, SC-7, SC-8, SC-11, SC-12, SC-13, SC-28, SC-31, SI-4	ISA 62443-3-3:2013 SR 3.1, SR 3.4, SR. 3.8, SR 4.1, SR 4.1, SR 4.2, SR 5.2				CIP-005-7-R1 CIP-005-7-R2 CIP-011-2-R1 CIP-012-1-R1 CIP-011-2-R1 CIP-011-3-R1	
2.N Disable Macros by Default	Establish software restriction policies to prevent the execution of unauthorized code, such as a system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default. If macros must be enabled in specific circumstances, establish a policy for authorized users to request that macros are enabled on specific assets. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.	**2.N Disable Macros by Default** A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.	PR.IP-1, PR.IP-3	ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h ARCHITECTURE-3m ARCHITECTURE-6c	NIST SP 800-53: CM-10, CM-11, SC-13	ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6	ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4			CIP-010-4-R1 CIP-010-4-R2	
2.O Document Device Configurations	Document and maintain baselines and current configuration details of critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodically review and update documentation.	**2.O Document Device Configurations** Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and	PR.IP-1	ASSET-3a ASSET-3d ARCHITECTURE-3e ARCHITECTURE-4c	NIST SP 800-53: CM-2, CM-6, CM-8	ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6	ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	SM-1a		CIP-010-4-R1	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
		updates are performed and tracked on a recurring basis.									
2.P Document & Maintain Network Topology	Document and maintain physical and logical network topology across critical IT and OT networks. Review and document any change to the topology.	**2.P Document & Maintain Network Topology** Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and OT networks. Periodic reviews and updates should be performed and tracked on a recurring basis.	PR.IP-1	ARCHITECTURE-1c ARCHITECTURE-1d	NIST SP 800-53: CM-2, CM-6, CM-8	ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6	ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	SM-1a		CIP-010-4-R1	
2.Q Hardware and Software Approval Process	Implement an administrative policy or automated process for critical IT and OT assets that requires approval before new hardware, firmware, or software/software version is installed or deployed, or before the asset is removed/decommissioned. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.	**2.Q Hardware and Software Approval Process** Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.	PR.IP-3	ASSET-4a ASSET-4g ASSET-5c ARCHITECTURE-1d ARCHITECTURE-4f ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h ARCHITECTURE-6c	NIST SP 800-53: CM-2, CM-3, CM-5, CM-6, CM-10, CM-11	ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6	ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	RA-19		CIP-010-4-R1	
2.R System Backups	Establish and maintain a documented system restoration plan, including processes to back up critical systems where deemed appropriate by the organization.	**2.R System Backups** All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). • Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, programmable controller (PLC) logic, engineering drawings, and tools.	PR.IP-4	RESPONSE-3a RESPONSE-3d RESPONSE-4a RESPONSE-4b RESPONSE-4c RESPONSE-4f	NIST SP 800-53: CP-6, CP-9, CP-10	ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4	ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3	SM-69, SM-70, SM-71, SM-72		CIP-009-6-R1 CIP-009-6-R2	
2.S Incident Response (IR) Plans	Establish, maintain, and regularly (at least annually) drill IT and OT cybersecurity incident response plans for both common and organizationally specific (e.g., by sector, locality) threat scenarios and TTPs. • Update incident response plans within a risk-informed time frame to	**2.S Incident Response (IR) Plans** Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-	PR.IP-9, PR.IP-10.	RESPONSE-3d RESPONSE-3g RESPONSE-3h	NIST SP 800-53: IR-3, IR-4, IR-8	ISA 62443-2-1:2009 4.3.2.5.3, 4.3.2.5.7, 4.3.4.5.1, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3	ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3	CM-1, CM-2, CM-3, CM-4, CM-5, CM-7, CM-8, CM-9, CM-10		CIP-003-8-R2 CIP-008-6-R1 CIP-008-6-R2 CIP-008-6-R3 CIP-009-6-R1 CIP-009-6-R2 CIP-009-6-R3	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
	incorporate lessons learned from the exercise or drill.	informed time frame following the lessons learned portion of any exercise or drill.									
2.T Log Collection	Collect and store time-synchronized access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) based on criticality for use in both detection and incident response activities (e.g., forensics). • OT: For OT assets where logs are non-standard or not available, collect network traffic and communications between those assets and other assets where feasible.	**2.T Log Collection** Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. • OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.	PR.PT-1	ACCESS-2i ACCESS-3c SITUATION-1a SITUATION-1b SITUATION-1c SITUATION-1d SITUATION-1f	NIST SP 800-53: AU-2, AU-3, AU-7, AU-9, AU-11	ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12	ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	NE-28a	6.5.1DER/LOG/REQ-01	CIP-006-6-R1 CIP-006-6-R2 CIP-007-6-R4	
2.U Secure Log Storage	Establish and maintain a process to protect logs for critical IT and OT assets from unauthorized access.	**2.U Secure Log Storage** Logs are stored in a central system, such as a security information and event management tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.	PR.PT-1	ACCESS-2a ACCESS-2c ARCHITECTURE-5a ARCHITECTURE-5b	NIST SP 800-53: AU-2, AU-3, AU-7, AU-9, AU-11	ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12	ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	NE-27a	DER/LOG/REQ-06	CIP-006-6-R1 CIP-006-6-R2 CIP-007-6-R4	
2.V Prohibit Connection of Unauthorized Devices	Establish and maintain policies and processes to reduce the probability that unauthorized media or hardware are connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun. • Define acceptable types of media and hardware and establish scanning requirements when appropriate for devices that have a storage component. • Establish validation and authorization steps when new devices are	**2.V Prohibit Connection of Unauthorized Devices** Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun. • OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions.	PR.PT-2	WORKFORCE-1e ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3d ARCHITECTURE-3g ARCHITECTURE-3h ARCHITECTURE-3m ARCHITECTURE-6a ARCHITECTURE-6c	NIST SP 800-53: MP-2, MP-7	ISA 62443-3-3:2013 SR 2.3	ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9	NE-36a		CIP-003-8-R2 CIP-007-6-R1 CIP-010-4-R4	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
	connected to ensure no unauthorized devices are connected. • OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions. • Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.										
2.W No Exploitable Services on the Internet	Implement a process to minimize the number of ports and services exposed to the Internet. • Prevent assets on the public internet from exposing services with known exploits. • Where these services must be exposed, document and implement appropriate compensating controls to prevent common forms of abuse and exploitation. • Disable unnecessary applications and network protocols on internet-facing assets.	**2.W No Exploitable Services on the Internet** Assets on the public internet expose no exploitable services, such as remote desktop protocol. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.	PR.PT-4	ARCHITECTURE-2e ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3d ARCHITECTURE-3h	NIST SP 800-53: AC-4, SC-7, SC-32, SC-39	ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3	NE-42a	DER/DSEC/REQ-01	CIP-005-7-R1 CIP-005-7-R2 CIP-005-7-R3 CIP-006-6-R1 CIP-012-1-R1	
2.X Limit OT Connections to Public Internet	Establish and implement a process to ensure OT assets are not placed on the public internet, unless explicitly required for operation. Document necessary exceptions and implement compensating controls for excepted assets to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary jump host, etc.).	**2.X Limit OT Connections to Public Internet** No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).	PR.PT-4	ARCHITECTURE-2a ARCHITECTURE-2b ARCHITECTURE-2c ARCHITECTURE-2d ARCHITECTURE-2e ARCHITECTURE-2f ARCHITECTURE-2g ARCHITECTURE-3a ARCHITECTURE-3b ARCHITECTURE-3h	NIST SP 800-53: AC-4, SC-7, SC-32, SC-39	ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3			CIP-005-7-R1 CIP-005-7-R2 CIP-005-7-R3 CIP-006-6-R1 CIP-012-1-R1	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
3.A Detecting Relevant Threats and TTPs	Maintain situational awareness of threats and cyber actor tactics, techniques, and procedures (TTPs) relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.	**3.A Detecting Relevant Threats and TTPs** Organizations document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.	ID.RA-3, DE.CM-1	THREAT-2a THREAT-2b THREAT-2d THREAT-2e SITUATION-1a SITUATION-1c SITUATION-2a SITUATION-2b SITUATION-2c SITUATION-2e SITUATION-2f	NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM3, RA-3, SC-5, SC-7, SI-4, SI-5, PM-12, PM-16	ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISA 62443-3-3:2013 SR 6.2	ISO/IEC 27001:2013 A.6.1.3, A.16.1.2, Clause 7.4	CM-1, CM-2, CM-3, CM-4, CM-5, CM-7, CM-8, CM-9, CM-10		CIP-005-7-R1 CIP-007-6-R4	
4.A Incident Reporting	Establish and maintain codified policy and procedures on when, to whom, and how to report all confirmed cybersecurity incidents to appropriate external entities.	**4.A Incident Reporting** Organizations maintain codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g., state/federal regulators or SRMA's as required, ISAC/ISAO, as well as CISA). • Known incidents are reported to CISA as well as other necessary parties within time frames directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).	RS.CO-2, RS.CO-4	RESPONSE-2g RESPONSE-3c RESPONSE-3f RESPONSE-5a RESPONSE-5c	NIST SP 800-53: IR-6	ISA 62443-2-1:2009 4.3.4.5.5		CM-1, CM-2, CM-3, CM-4, CM-5, CM-7, CM-8, CM-9, CM-10		CIP-003-8-R2 CIP-008-6-R1 CIP-008-6-R2 CIP-008-6-R4	
4.B Vulnerability Disclosure/Reporting	Establish and maintain a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) the organization's security teams of vulnerable, misconfigured, or otherwise exploitable assets. Acknowledge and respond to valid submissions in a timely manner, taking into account the completeness and complexity of the vulnerability. Mitigate validated and exploitable weaknesses consistent with their severity. • Protect security researchers sharing vulnerabilities discovered in good faith under Safe Harbor rules.	**4.B Vulnerability Disclosure/Reporting** Consistent with NIST SP 800-53 Revision 5, organizations maintain a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) organizations' security teams of vulnerable, misconfigured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity. • Security researchers sharing vulnerabilities discovered in good faith are protected under Safe Harbor rules. • In instances where vulnerabilities are validated and disclosed, public	RS.AN-5	THREAT-1d THREAT-1g THREAT-1m	NIST SP 800-53: RA-5		ISO/IEC 29147, 30111	CM-1, CM-2, CM-3, CM-4, CM-5, CM-7, CM-8, CM-9, CM-10		CIP-007-6-R2 CIP-010-4-R3 CIP-010-4-R4 CIP-013-2-R1	

NOTE: Informative References do not represent equivalent or interchangeable practices. See Cautions on Using the Informative References on page 2 before reviewing this table.

Name	Distribution and DER Baseline	Voluntary Cybersecurity Frameworks and Guidelines			Voluntary Standards for System Implementation or Manufacturing					Regulatory Standards for Select Energy Systems	
		DHS CISA CPG Ver. 1.0.1 Recommended Action Text	NIST CSF Ver. 1.1	DOE C2M2 Ver. 2.1	NIST SP 800-53	ISA 62443	ISO/IEC 27001:2013	IEEE 1547.3	SunSpec DER Cybersecurity Phase 1	NERC CIP	DHS TSA SD-02D
	• In instances where vulnerabilities are validated and disclosed, give public acknowledgement to the researcher who originally submitted the notification. • Determine appropriate public disclosure steps (including not disclosing) using a risk-informed decision process that considers the possibility that the vulnerability may still exist in other distribution systems.	acknowledgement is given to the researcher who originally submitted the notification.									
4.C Deploy Security.TXT Files	Ensure that public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.	**4.C Deploy Security.TXT Files** All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116	RS.AN-5	THREAT-1m	NIST SP 800-53 Rev. 4 SI-5, PM-15			CM-1, CM-2, CM-3, CM-4, CM-5, CM-7, CM-8, CM-9, CM-10		CIP-007-6-R2 CIP-010-4-R3 CIP-010-4-R4 CIP-013-2-R1	III D I e
5.A Incident Planning and Preparedness	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.	**5.A Incident Planning and Preparedness** Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.	RC.RP-1, PR.IP-9, PR.IP-10	RESPONSE-3a RESPONSE-3b RESPONSE-3d RESPONSE-3e RESPONSE-4a RESPONSE-4b RESPONSE-4c RESPONSE-4d RESPONSE-4e RESPONSE-4f RESPONSE-4g RESPONSE-4h RESPONSE-4l	NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8			CM-1, CM-2, CM-3, CM-4, CM-5, CM-7, CM-8, CM-9, CM-10		CIP-003-8-R2 CIP-008-6-R1 CIP-008-6-R3 CIP-009-6-R1 CIP-009-6-R2 CIP-009-6-R3	