NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: NERC Reliability Standards for the Bulk Electric Systems of North America (complete set) Oct 2024
Focal Document URL: https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-us-nerc-cip-2024.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-002-5.1a R1	N/A	Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [Violation Risk Factor: High][Time Horizon: Operations Planning] I. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-002-5.1a 1.1	N/A	Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
CIP-002-5.1a 1.2	N/A	Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
CIP-002-5.1a 1.3	N/A	Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
CIP-002-5.1a R2	N/A	The Responsible Entity shall: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-002-5.1a 2.1	N/A	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CIP-002-5.1a 2.2	N/A	Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CIP-003-8 R1	N/A	Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CIP-003-8 1.1	N/A	For its high impact and medium impact BES Cyber Systems, if any:	Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
CIP-003-8 1.1.1	N/A	Personnel and training (CIP-004);	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
CIP-003-8 1.1.2	N/A	Electronic Security Perimeters (CIP-005) including Interactive Remote Access;	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CIP-003-8 1.1.2	N/A	Electronic Security Perimeters (CIP-005) including Interactive Remote Access;	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
CIP-003-8 1.1.3	N/A	Physical security of BES Cyber Systems (CIP-006);	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
CIP-003-8 1.1.4	N/A	System security management (CIP-007);	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
CIP-003-8 1.1.4	N/A	System security management (CIP-007);	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
CIP-003-8 1.1.5	N/A	Incident reporting and response planning (CIP-008);	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
CIP-003-8 1.1.6	N/A	Recovery plans for BES Cyber Systems (CIP-009);	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CIP-003-8 1.1.7	N/A	Configuration change management and vulnerability assessments (CIP-010);	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CIP-003-8 1.1.7	N/A	Configuration change management and vulnerability assessments (CIP-010);	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CIP-003-8 1.1.7	N/A	Configuration change management and vulnerability assessments (CIP-010);	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
CIP-003-8 1.1.8	N/A	Information protection (CIP-011); and	Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
CIP-003-8 1.1.9	N/A	Declaring and responding to CIP Exceptional Circumstances.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
CIP-003-8 1.2	N/A	For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-003-8 1.2.1	N/A	Cyber security awareness;	Functional	subset of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
CIP-003-8 1.2.2	N/A	Physical security controls;	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
CIP-003-8 1.2.3	N/A	Electronic access controls;	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CIP-003-8 1.2.4	N/A	Cyber Security Incident response;	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
CIP-003-8 1.2.5	N/A	Transient Cyber Assets and Removable Media malicious code risk mitigation; and	Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
CIP-003-8 1.2.6	N/A	Declaring and responding to CIP Exceptional Circumstances.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
CIP-003-8 R2	N/A	Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
CIP-003-8 R3	N/A	Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	8	
CIP-003-8 R4	N/A	The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	Functional	subset of	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	10	
CIP-004-7 R1	N/A	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-7 Table R1 – Security Awareness Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-004-7 1.1	CIP-004-7 Table R1 – Security Awareness Program	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
CIP-004-7 R2	N/A	Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-7 Table R2 – Cyber Security Training Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
CIP-004-7 R2	N/A	Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-7 Table R2 – Cyber Security Training Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
CIP-004-7 2.1	CIP-004-7 Table R2 – Cyber Security Training Program	Training content on:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-004-7 2.1.1	CIP-004-7 Table R2 – Cyber Security Training Program	Cybersecurity policies;	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.1.2	CIP-004-7 Table R2 – Cyber Security Training Program	Physical access controls;	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.1.3	CIP-004-7 Table R2 – Cyber Security Training Program	Electronic access controls;	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.1.4	CIP-004-7 Table R2 – Cyber Security Training Program	The visitor control program;	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.1.5	CIP-004-7 Table R2 – Cyber Security Training Program	Handling of BES Cyber System Information and its storage;	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.1.6	CIP-004-7 Table R2 – Cyber Security Training Program	Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.1.7	CIP-004-7 Table R2 – Cyber Security Training Program	Recovery plans for BES Cyber Systems;	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.1.8	CIP-004-7 Table R2 – Cyber Security Training Program	Response to Cyber Security Incidents; and	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.1.9	CIP-004-7 Table R2 – Cyber Security Training Program	Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media	Functional	subset of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
CIP-004-7 2.2	CIP-004-7 Table R2 – Cyber Security Training Program	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
CIP-004-7 2.2	CIP-004-7 Table R2 – Cyber Security Training Program	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
CIP-004-7 2.2	CIP-004-7 Table R2 – Cyber Security Training Program	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
CIP-004-7 2.3	CIP-004-7 Table R2 – Cyber Security Training Program	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
CIP-004-7 R3	N/A	Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-7 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
CIP-004-7 R3	N/A	Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-7 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
CIP-004-7 3.1	CIP-004-7 Table R3 – Personnel Risk Assessment Program	Process to confirm identity.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
CIP-004-7 3.2	CIP-004-7 Table R3 – Personnel Risk Assessment Program	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: End note - If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
CIP-004-7 3.2.1	CIP-004-7 Table R3 – Personnel Risk Assessment Program	current residence, regardless of duration; and	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
CIP-004-7 3.2.2	CIP-004-7 Table R3 – Personnel Risk Assessment Program	other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
CIP-004-7 3.3	CIP-004-7 Table R3 – Personnel Risk Assessment Program	Criteria or process to evaluate criminal history records checks for authorizing access.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
CIP-004-7 3.4	CIP-004-7 Table R3 – Personnel Risk Assessment Program	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
CIP-004-7 3.5	CIP-004-7 Table R3 – Personnel Risk Assessment Program	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
CIP-004-7 R4	N/A	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CIP-004-7 4.1	CIP-004-7 Table R4 – Access Management Program	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
CIP-004-7 4.1.1	CIP-004-7 Table R4 – Access Management Program	Electronic access; and	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CIP-004-7 4.1.2	CIP-004-7 Table R4 – Access Management Program	Unescorted physical access into a Physical Security Perimeter	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
CIP-004-7 4.1.2	CIP-004-7 Table R4 – Access Management Program	Unescorted physical access into a Physical Security Perimeter	Functional	Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-004-7 4.2	CIP-004-7 Table R4 – Access Management Program	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records	Functional	subset of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	
CIP-004-7 4.3	CIP-004-7 Table R4 – Access Management Program	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	8	
CIP-004-7 R5	N/A	Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-7 Table R5 – Access Revocation. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].	Functional	subset of	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	10	
CIP-004-7 5.1	CIP-004-7 Table R5 – Access Revocation	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	Functional	subset of	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	10	
CIP-004-7 5.2	CIP-004-7 Table R5 – Access Revocation	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Functional	subset of	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	10	
CIP-004-7 5.3	CIP-004-7 Table R5 – Access Revocation	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	8	
CIP-004-7 5.3	CIP-004-7 Table R5 – Access Revocation	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Functional	Intersects With	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	8	
CIP-004-7 5.4	CIP-004-7 Table R5 – Access Revocation	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	8	
CIP-004-7 R6	N/A	Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CIP-004-7 6.1	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:	Functional	subset of	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	10	
CIP-004-7 6.1.1	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	Provisioned electronic access to electronic BCSI; and	Functional	subset of	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
CIP-004-7 6.1.2	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	Provisioned physical access to physical BCSI.	Functional	subset of	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
CIP-004-7 6.1.2	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	Provisioned physical access to physical BCSI.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	
CIP-004-7 6.2	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	8	
CIP-004-7 6.2.1	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	have an authorization record; and	Functional	subset of	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	
CIP-004-7 6.2.2	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Functional	subset of	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	
CIP-004-7 6.3	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Functional	subset of	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	10	
CIP-004-7 6.3	CIP-004-7 Table R6 – Access Management for BES Cyber System Information	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	8	
CIP-005-7 R1	N/A	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-7 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-005-7 1.1	CIP-005-7 Table R1 – Electronic Security Perimeter	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
CIP-005-7 1.2	CIP-005-7 Table R1 – Electronic Security Perimeter	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
CIP-005-7 1.3	CIP-005-7 Table R1 – Electronic Security Perimeter	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	8	
CIP-005-7 1.4	CIP-005-7 Table R1 – Electronic Security Perimeter	Where technically feasible, perform authentication when establishing Dialup Connectivity with applicable Cyber Assets.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	8	
CIP-005-7 1.5	CIP-005-7 Table R1 – Electronic Security Perimeter	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
CIP-005-7 1.5	CIP-005-7 Table R1 – Electronic Security Perimeter	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
CIP-005-7 R2	N/A	Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-7 Table R2 –Remote Access Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-005-7 2.1	CIP-005-7 Table R2 – Remote Access Management	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Functional	subset of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	
CIP-005-7 2.2	CIP-005-7 Table R2 – Remote Access Management	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	Functional	Intersects With	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	8	
CIP-005-7 2.3	CIP-005-7 Table R2 – Remote Access Management	Require multi-factor authentication for all Interactive Remote Access sessions.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	8	
CIP-005-7 2.3	CIP-005-7 Table R2 – Remote Access Management	Require multi-factor authentication for all Interactive Remote Access sessions.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
CIP-005-7 2.4	CIP-005-7 Table R2 – Remote Access Management	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
CIP-005-7 2.4	CIP-005-7 Table R2 – Remote Access Management	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Functional	Intersects With	Third-Party Remote Access Governance	NET-14.6	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5	
CIP-005-7 2.5	CIP-005-7 Table R2 – Remote Access Management	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Functional	Intersects With	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5	
CIP-005-7 2.5	CIP-005-7 Table R2 – Remote Access Management	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Functional	Intersects With	Third-Party Remote Access Governance	NET-14.6	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5	
CIP-005-7 2.5	CIP-005-7 Table R2 – Remote Access Management	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Functional	Intersects With	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.	5	
CIP-005-7 R3	N/A	Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-005-7 3.1	CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS	Have one or more method(s) to determine authenticated vendor initiated remote connections.	Functional	Intersects With	Remote Maintenance Pre-Approval	MNT-05.5	Mechanisms exist to require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions.	5	
CIP-005-7 3.1	CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS	Have one or more method(s) to determine authenticated vendor initiated remote connections.	Functional	Intersects With	Third-Party Remote Access Governance	NET-14.6	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5	
CIP-005-7 3.2	CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS	Have one or more method(s) to terminate authenticated vendor initiated remote connections and control the ability to reconnect.	Functional	Intersects With	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5	
CIP-005-7 3.2	CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS	Have one or more method(s) to terminate authenticated vendor initiated remote connections and control the ability to reconnect.	Functional	Intersects With	Third-Party Remote Access Governance	NET-14.6	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5	
CIP-005-7 3.2	CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS	Have one or more method(s) to terminate authenticated vendor initiated remote connections and control the ability to reconnect.	Functional	Intersects With	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.	5	
CIP-006-6 R1	N/A	Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].	Functional	subset of	Physical Security Plan (PSP)	PES-01.1	Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	10	
CIP-006-6 1.1	CIP-006-6 Table R1 – Physical Security Plan	Define operational or procedural controls to restrict physical access.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
CIP-006-6 1.1	CIP-006-6 Table R1 – Physical Security Plan	Define operational or procedural controls to restrict physical access.	Functional	subset of	Physical Security Plan (PSP)	PES-01.1	Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	10	
CIP-006-6 1.1	CIP-006-6 Table R1 – Physical Security Plan	Define operational or procedural controls to restrict physical access.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
CIP-006-6 1.2	CIP-006-6 Table R1 – Physical Security Plan	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	Functional	Intersects With	Zone-Based Physical Security	PES-01.2	Mechanisms exist to implement a zone-based approach to physical security.	5	
CIP-006-6 1.2	CIP-006-6 Table R1 – Physical Security Plan	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	8	
CIP-006-6 1.2	CIP-006-6 Table R1 – Physical Security Plan	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	8	
CIP-006-6 1.2	CIP-006-6 Table R1 – Physical Security Plan	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	Functional	Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	8	
CIP-006-6 1.3	CIP-006-6 Table R1 – Physical Security Plan	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	Functional	subset of	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	10	
CIP-006-6 1.3	CIP-006-6 Table R1 – Physical Security Plan	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
CIP-006-6 1.3	CIP-006-6 Table R1 – Physical Security Plan	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	Functional	Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
CIP-006-6 1.4	CIP-006-6 Table R1 – Physical Security Plan	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	Functional	Intersects With	Unauthorized Activities	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	5	
CIP-006-6 1.4	CIP-006-6 Table R1 – Physical Security Plan	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	
CIP-006-6 1.4	CIP-006-6 Table R1 – Physical Security Plan	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	Functional	subset of	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	
CIP-006-6 1.5	CIP-006-6 Table R1 – Physical Security Plan	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
CIP-006-6 1.5	CIP-006-6 Table R1 – Physical Security Plan	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5	
CIP-006-6 1.5	CIP-006-6 Table R1 – Physical Security Plan	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	8	
CIP-006-6 1.6	CIP-006-6 Table R1 – Physical Security Plan	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	Functional	subset of	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-006-6 1.7	CIP-006-6 Table R1 – Physical Security Plan	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	
CIP-006-6 1.7	CIP-006-6 Table R1 – Physical Security Plan	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	8	
CIP-006-6 1.8	CIP-006-6 Table R1 – Physical Security Plan	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	Functional	subset of	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	
CIP-006-6 1.9	CIP-006-6 Table R1 – Physical Security Plan	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	8	
CIP-006-6 1.9	CIP-006-6 Table R1 – Physical Security Plan	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	
CIP-006-6 1.10	CIP-006-6 Table R1 – Physical Security Plan	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	3	
CIP-006-6 1.10	CIP-006-6 Table R1 – Physical Security Plan	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	Functional	subset of	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	10	
CIP-006-6 1.10	CIP-006-6 Table R1 – Physical Security Plan	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
CIP-006-6 1.10	CIP-006-6 Table R1 – Physical Security Plan	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
CIP-006-6 R2	N/A	Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]	Functional	subset of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	
CIP-006-6 2.1	CIP-006-6 Table R2 – Visitor Control Program	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	Functional	Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	8	
CIP-006-6 2.2	CIP-006-6 Table R2 – Visitor Control Program	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	Functional	subset of	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	
CIP-006-6 2.2	CIP-006-6 Table R2 – Visitor Control Program	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	Functional	Intersects With	Identification Requirement	PES-06.2	Physical access control mechanisms exist to requires at least one (1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.	8	
CIP-006-6 2.3	CIP-006-6 Table R2 – Visitor Control Program	Retain visitor logs for at least ninety calendar days.	Functional	subset of	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	10	
CIP-006-6 R3	N/A	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5	
CIP-006-6 3.1	CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5	
CIP-007-6 R1	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-007-6 1.1	CIP-007-6 Table R1– Ports and Services	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Functional	subset of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
CIP-007-6 1.2	CIP-007-6 Table R1– Ports and Services	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Functional	Intersects With	Port & Input / Output (I/O) Device Access	END-12	Mechanisms exist to physically disable or remove unnecessary connection ports or input/output devices from sensitive systems.	8	
CIP-007-6 1.3	CIP-007-6 Table R1– Ports and Services	A patch management process for tracking, evaluating, and installing cybersecurity patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-007-6 1.3	CIP-007-6 Table R1 – Ports and Services	A patch management process for tracking, evaluating, and installing cybersecurity patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
CIP-007-6 R2	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-007-6 2.1	CIP-007-6 Table R2 – Security Patch Management	A patch management process for tracking, evaluating, and installing cybersecurity patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
CIP-007-6 2.2	CIP-007-6 Table R2 – Security Patch Management	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
CIP-007-6 2.3	CIP-007-6 Table R2 – Security Patch Management	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Functional	subset of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
CIP-007-6 2.3	CIP-007-6 Table R2 – Security Patch Management	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
CIP-007-6 2.4	CIP-007-6 Table R2 – Security Patch Management	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Functional	subset of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
CIP-007-6 2.4	CIP-007-6 Table R2 – Security Patch Management	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
CIP-007-6 R3	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-007-6 3.1	CIP-007-6 Table R3 – Malicious Code Prevention	Deploy method(s) to deter, detect, or prevent malicious code.	Functional	subset of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
CIP-007-6 3.1	CIP-007-6 Table R3 – Malicious Code Prevention	Deploy method(s) to deter, detect, or prevent malicious code.	Functional	Intersects With	Malicious Link & File Protections	END-14.5	Automated mechanisms exist to detect malicious links and/or files in communications and prevent users from accessing those malicious links and/or files.	3	
CIP-007-6 3.2	CIP-007-6 Table R3 – Malicious Code Prevention	Mitigate the threat of detected malicious code.	Functional	subset of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
CIP-007-6 3.3	CIP-007-6 Table R3 – Malicious Code Prevention	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
CIP-007-6 3.3	CIP-007-6 Table R3 – Malicious Code Prevention	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Functional	Intersects With	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	8	
CIP-007-6 R4	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-007-6 4.1	CIP-007-6 Table R4 – Security Event Monitoring	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	8	
CIP-007-6 4.1	CIP-007-6 Table R4 – Security Event Monitoring	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	
CIP-007-6 4.1.1	CIP-007-6 Table R4 – Security Event Monitoring	Detected successful login attempts;	Functional	subset of	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	10	
CIP-007-6 4.1.2	CIP-007-6 Table R4 – Security Event Monitoring	Detected failed access attempts and failed login attempts;	Functional	subset of	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	10	
CIP-007-6 4.1.3	CIP-007-6 Table R4 – Security Event Monitoring	Detected malicious code.	Functional	subset of	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	10	
CIP-007-6 4.2	CIP-007-6 Table R4 – Security Event Monitoring	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):	Functional	subset of	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
CIP-007-6 4.2.1	CIP-007-6 Table R4 – Security Event Monitoring	Detected malicious code from Part 4.1; and	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	8	
CIP-007-6 4.2.2	CIP-007-6 Table R4 – Security Event Monitoring	Detected failure of Part 4.1 event logging.	Functional	subset of	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	10	
CIP-007-6 4.3	CIP-007-6 Table R4 – Security Event Monitoring	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Functional	subset of	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-007-6 4.4	CIP-007-6 Table R4 – Security Event Monitoring	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Functional	Intersects With	Event Log Analysis & Triage	MON-17	Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes.	8	
CIP-007-6 R5	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-007-6 5.1	CIP-007-6 Table R5 – System Access Control	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CIP-007-6 5.1	CIP-007-6 Table R5 – System Access Control	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
CIP-007-6 5.2	CIP-007-6 Table R5 – System Access Control	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Functional	subset of	User & Service Account Inventories	IAC-01.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	10	
CIP-007-6 5.3	CIP-007-6 Table R5 – System Access Control	Identify individuals who have authorized access to shared accounts.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
CIP-007-6 5.3	CIP-007-6 Table R5 – System Access Control	Identify individuals who have authorized access to shared accounts.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
CIP-007-6 5.4	CIP-007-6 Table R5 – System Access Control	Change known default passwords, per Cyber Asset capability.	Functional	subset of	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	10	
CIP-007-6 5.5	CIP-007-6 Table R5 – System Access Control	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-007-6 5.5.1	CIP-007-6 Table R5 – System Access Control	Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and	Functional	subset of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
CIP-007-6 5.5.2	CIP-007-6 Table R5 – System Access Control	Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.	Functional	subset of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
CIP-007-6 5.6	CIP-007-6 Table R5 – System Access Control	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
CIP-007-6 5.7	CIP-007-6 Table R5 – System Access Control	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Functional	Intersects With	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	8	
CIP-008-6 R1	N/A	Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].	Functional	subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
CIP-008-6 1.1	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	8	
CIP-008-6 1.1	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
CIP-008-6 1.1	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8	
CIP-008-6 1.1	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
CIP-008-6 1.2	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	One or more processes:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-008-6 1.2.1	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	That include criteria to evaluate and define attempts to compromise;	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
CIP-008-6 1.2.1	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	That include criteria to evaluate and define attempts to compromise;	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	3	
CIP-008-6 1.2.1	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	That include criteria to evaluate and define attempts to compromise;	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
CIP-008-6 1.2.2	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and	Functional	subset of	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	10	
CIP-008-6 1.2.2	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	
CIP-008-6 1.2.3	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	To provide notification per Requirement R4	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-008-6 1.3	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Functional	subset of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
CIP-008-6 1.3	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	8	
CIP-008-6 1.4	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	Incident handling procedures for Cyber Security Incidents.	Functional	subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
CIP-008-6 1.4	CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	Incident handling procedures for Cyber Security Incidents.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
CIP-008-6 R2	N/A	Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].	Functional	subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-008-6 2.1	CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Functional	subset of	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	10	
CIP-008-6 2.2	CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Functional	subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
CIP-008-6 2.3	CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	3	
CIP-008-6 2.3	CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	8	
CIP-008-6 R3	N/A	Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].	Functional	subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
CIP-008-6 3.1	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
CIP-008-6 3.1.1	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	Document any lessons learned or document the absence of any lessons learned;	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8	
CIP-008-6 3.1.2	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and	Functional	subset of	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	10	
CIP-008-6 3.1.2	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8	
CIP-008-6 3.1.3	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	3	
CIP-008-6 3.1.3	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	3	
CIP-008-6 3.2	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan:	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
CIP-008-6 3.2.1	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	Update the Cyber Security Incident response plan(s); and	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	3	
CIP-008-6 3.2.2	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	3	
CIP-008-6 3.2.2	CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication	Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	3	
CIP-008-6 R4	N/A	Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC),1 or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].	Functional	subset of	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	10	
CIP-008-6 4.1	CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:	Functional	subset of	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	10	
CIP-008-6 4.1.1	CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents	The functional impact;	Functional	subset of	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	10	
CIP-008-6 4.1.2	CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents	The attack vector used; and	Functional	subset of	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	10	
CIP-008-6 4.1.3	CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents	The level of intrusion that was achieved or attempted.	Functional	subset of	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	10	
CIP-008-6 4.2	CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Functional	subset of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-008-6 4.2	CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
CIP-008-6 4.2	CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	8	
CIP-008-6 4.3	CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Functional	subset of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
CIP-009-6 R1	N/A	Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CIP-009-6 1.1	CIP-009-6 Table R1 – Recovery Plan Specifications	Conditions for activation of the recovery plan(s).	Functional	Intersects With	Recovery Operations Criteria	BCD-01.5	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recover (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
CIP-009-6 1.2	CIP-009-6 Table R1 – Recovery Plan Specifications	Roles and responsibilities of responders.	Functional	subset of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
CIP-009-6 1.3	CIP-009-6 Table R1 – Recovery Plan Specifications	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	Functional	subset of	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	
CIP-009-6 1.4	CIP-009-6 Table R1 – Recovery Plan Specifications	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Functional	subset of	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	
CIP-009-6 1.4	CIP-009-6 Table R1 – Recovery Plan Specifications	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	8	
CIP-009-6 1.5	CIP-009-6 Table R1 – Recovery Plan Specifications	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Functional	subset of	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	10	
CIP-009-6 R2	N/A	Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CIP-009-6 2.1	CIP-009-6 Table R2 – Recovery Plan Implementation and Testing	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Functional	subset of	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
CIP-009-6 2.2	CIP-009-6 Table R2 – Recovery Plan Implementation and Testing	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
CIP-009-6 2.3	CIP-009-6 Table R2 – Recovery Plan Implementation and Testing	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Functional	subset of	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
CIP-009-6 R3	N/A	Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CIP-009-6 3.1	CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication	No later than 90 calendar days after completion of a recovery plan test or actual recovery:	Functional	subset of	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
CIP-009-6 3.1.1	CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication	Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
CIP-009-6 3.1.2	CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication	Update the recovery plan based on any documented lessons learned associated with the plan; and	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
CIP-009-6 3.1.3	CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication	Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services) (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.	3	
CIP-009-6 3.2	CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:	Functional	Intersects With	Contingency Planning Components	BCD-06.1	Mechanisms exist to identify components that potentially impact the organization's ability to execute contingency plans, including changes to: (1) Personnel roles; (2) Business processes (including the use of third-party services); (3) Deployed technologies; (4) Data repositories and/or data flows; and/or (5) Physical infrastructure.	8	
CIP-009-6 3.2.1	CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication	Update the recovery plan; and	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services) (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.	5	
CIP-009-6 3.2.2	CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication	Notify each person or group with a defined role in the recovery plan of the updates.	Functional	Intersects With	Contingency Plan Update Notifications	BCD-06.2	Mechanisms exist to keep stakeholders informed of changes to contingency plans.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-010-3 R1	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-4 Table R1 – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CIP-010-4 1.1	CIP-010-4 Table R1 – Configuration Change Management	Develop a baseline configuration, individually or by group, which shall include the following items:	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
CIP-010-4 1.1.1	CIP-010-4 Table R1 – Configuration Change Management	Operating system(s) (including version) or firmware where no independent operating system exists;	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
CIP-010-4 1.1.2	CIP-010-4 Table R1 – Configuration Change Management	Any commercially available or open-source application software (including version) intentionally installed;	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
CIP-010-4 1.1.3	CIP-010-4 Table R1 – Configuration Change Management	Any custom software installed;	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
CIP-010-4 1.1.4	CIP-010-4 Table R1 – Configuration Change Management	Any logical network accessible ports; and	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
CIP-010-4 1.1.5	CIP-010-4 Table R1 – Configuration Change Management	Any security patches applied.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
CIP-010-4 1.2	CIP-010-4 Table R1 – Configuration Change Management	Authorize and document changes that deviate from the existing baseline configuration.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	8	
CIP-010-4 1.3	CIP-010-4 Table R1 – Configuration Change Management	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	
CIP-010-4 1.4	CIP-010-4 Table R1 – Configuration Change Management	For a change that deviates from the existing baseline configuration:	Functional	subset of	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	10	
CIP-010-4 1.4.1	CIP-010-4 Table R1 – Configuration Change Management	Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;	Functional	subset of	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	10	
CIP-010-4 1.4.2	CIP-010-4 Table R1 – Configuration Change Management	Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
CIP-010-4 1.4.3	CIP-010-4 Table R1 – Configuration Change Management	Document the results of the verification.	Functional	subset of	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	10	
CIP-010-4 1.5	CIP-010-4 Table R1 – Configuration Change Management	Where technically feasible, for each change that deviates from the existing baseline configuration:	Functional	subset of	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	10	
CIP-010-4 1.5.1	CIP-010-4 Table R1 – Configuration Change Management	Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
CIP-010-4 1.5.2	CIP-010-4 Table R1 – Configuration Change Management	Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
CIP-010-4 1.6	CIP-010-4 Table R1 – Configuration Change Management	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:	Functional	subset of	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	10	
CIP-010-4 1.6.1	CIP-010-4 Table R1 – Configuration Change Management	Verify the identity of the software source; and	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
CIP-010-4 1.6.1	CIP-010-4 Table R1 – Configuration Change Management	Verify the identity of the software source; and	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
CIP-010-4 1.6.2	CIP-010-4 Table R1 – Configuration Change Management	Verify the integrity of the software obtained from the software source.	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
CIP-010-4 R2	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-010-4 2.1	CIP-010-4 Table R2 – Configuration Monitoring	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CIP-010-4 2.1	CIP-010-4 Table R2 – Configuration Monitoring	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	
CIP-010-4 R3	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 Table R3– Vulnerability Assessments. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-010-4 3.1	CIP-010-4 Table R3 – Vulnerability Assessments	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	
CIP-010-4 3.2	CIP-010-4 Table R3 – Vulnerability Assessments	Where technically feasible, at least once every 36 calendar months:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-010-4 3.2.1	CIP-010-4 Table R3 – Vulnerability Assessments	Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-010-4 3.2.2	CIP-010-4 Table R3 – Vulnerability Assessments	Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
CIP-010-4 3.3	CIP-010-4 Table R3 – Vulnerability Assessments	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
CIP-010-4 3.4	CIP-010-4 Table R3 – Vulnerability Assessments	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
CIP-011-3 R1	N/A	Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in CIP-011-3 Table R1 – Information Protection Program that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
CIP-011-3 1.1	CIP-011-3 Table R1 – Information Protection Program	Method(s) to identify BCSI.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
CIP-011-3 1.2	CIP-011-3 Table R1 – Information Protection Program	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
CIP-011-3 1.2	CIP-011-3 Table R1 – Information Protection Program	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	5	
CIP-011-3 1.2	CIP-011-3 Table R1 – Information Protection Program	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
CIP-011-3 1.2	CIP-011-3 Table R1 – Information Protection Program	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Functional	Intersects With	Enterprise Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Enterprise Device Management (EDM) controls.	8	
CIP-011-3 R2	N/A	Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-011-3 2.1	CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
CIP-011-3 2.2	CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
CIP-013-2 R1	N/A	Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	Functional	subset of	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	
CIP-013-2 1.1	N/A	One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
CIP-013-2 1.2	N/A	One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-013-2 1.2.1	N/A	Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5	
CIP-013-2 1.2.1	N/A	Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
CIP-013-2 1.2.2	N/A	Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	
CIP-013-2 1.2.2	N/A	Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
CIP-013-2 1.2.3	N/A	Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;	Functional	Intersects With	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	3	
CIP-013-2 1.2.4	N/A	Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;	Functional	Intersects With	Disclosure of Vulnerabilities	TDA-02.11	Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including: (1) A description of the vulnerability(ies); (2) Affected product(s) and/or service(s); (3) Potential impact of the vulnerability(ies); (4) Severity of the vulnerability(ies); and (5) Guidance to remediate the vulnerability(ies).	3	
CIP-013-2 1.2.5	N/A	Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	3	
CIP-013-2 1.2.6	N/A	Coordination of controls for vendor-initiated remote access.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	3	
CIP-013-2 R2	N/A	Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	Functional	equal	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	
CIP-013-2 R3	N/A	Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-014-3 R1	N/A	Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. [VRF: High; Time-Horizon: Long-term Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 1.1	N/A	Subsequent risk assessments shall be performed: • At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or • At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 1.2	N/A	The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 R2	N/A	Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. [VRF: Medium; Time-Horizon: Long-term Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 2.1	N/A	Each Transmission Owner shall select an unaffiliated verifying entity that is either: • A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or • An entity that has transmission planning or analysis experience.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 2.2	N/A	The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 2.3	N/A	If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation: • Modify its identification under Requirement R1 consistent with the recommendation; or • Document the technical basis for not modifying the identification in accordance with the recommendation.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 2.4	N/A	Each Transmission Owner shall implement procedures, such as the use of nondisclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 R3	N/A	For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. [VRF: Lower; Time- Horizon: Long-term Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 3.1	N/A	If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 R4	N/A	Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: [VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 4.1	N/A	Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 4.2	N/A	Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 4.3	N/A	Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 R5	N/A	Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: [VRF: High; Time-Horizon: Long-term Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 5.1	N/A	Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 5.2	N/A	Law enforcement contact and coordination information.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 5.3	N/A	A timeline for executing the physical security enhancements and modifications specified in the physical security plan.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 5.4	N/A	Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CIP-014-3 R6	N/A	Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. [VRF: Medium; Time-Horizon: Long-term Planning]	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 6.1	N/A	Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following: • An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification. • An entity or organization approved by the ERO. • A governmental agency with physical security expertise. • An entity or organization with demonstrated law enforcement, government, or military physical security expertise.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 6.2	N/A	The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 6.3	N/A	If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation: • Modify its evaluation or security plan(s) consistent with the recommendation; or • Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
CIP-014-3 6.4	N/A	Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	