Version 5	Applicability															Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
002-5 R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: 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. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. 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).															MC	**002-3 R2.** Critical Asset Identification The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary. **002-3 R3.** Critical Cyber Asset Identification Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a control center; or, R3.3. The Cyber Asset is dial-up accessible.
002-5 R2. The Responsible Entity shall: 2.1 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 2.2 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.															MC	**002-3 R4.** Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Version 5	Applicability															Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
003-5 R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, 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: 1.1 Personnel & Training (CIP-004); 1.2 Electronic Security Perimeters (CIP-005) Including interactive Remote Access; 1.3 Physical security of BES Cyber Systems (CIP-006); 1.4 System security management (CIP-007); 1.5 Incident Reporting and response planning (CIP-008); 1.6 Recovery plans for BES Cyber Systems (CIP-009); 1.7 Configuration change management and vulnerability assessments (CIP-010); 1.8 Information protection (CIP-011); and 1.9 Declaring and responding to CIP Exceptional Circumstances.		X		X											MC	**003-3 R1.** Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following: R1.1 The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations. R1.3 Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.
003-5 R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: 2.1 Cyber security awareness; 2.2 Physical security controls; 2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and 2.4 Incident response to a Cyber Security Incident. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.									X						MC	**003-3 R1.** Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following: R1.1 The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations. R1.3 Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.
003-5 R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	X			X					X						MC	**003-3 R2.** Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3. R2.1. The senior manager shall be identified by name, title, and date of designation. R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.
003-5 R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, 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.	X			X					X						MC	**003-3 R2.** R2.3. Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager. R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

Version 5	Applicability															Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP			
004-5 R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-5 Table R1 – Security Awareness Program. 1.1 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.	X			X												MC	**004-3 R1.** Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g., emails, memos, computer based training, etc.); • Indirect communications (e.g., posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).
004-5 R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-5 Table R2 – Cyber Security Training Program. 2.1 Training content on: 2.1.1 Cyber security policies; 2.1.2 Physical access controls; 2.1.3 Electronic access controls; 2.1.4 The visitor control program; 2.1.5 Handling of BES Cyber System Information and its storage; 2.1.6 Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7 Recovery plans for BES Cyber Systems; 2.1.8 Response to Cyber Security Incidents; and 2.1.9 Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets. 2.2 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. 2.3 Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	X						X			X	X					MC	**004-3 R2.** Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary. R2.1 This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency. R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities: R2.2.1 The proper use of Critical Cyber Assets; R2.2.2 Physical and electronic access controls to Critical Cyber Assets; R2.2.3 The proper handling of Critical Cyber Asset information; and R2.2.4 Action plans and procedures to recover or re-establish Critical Cyber Assets and access there to following a Cyber Security Incident.
004-5 R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs 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-004-5 Table R3 – Personnel Risk Assessment Program. 3.1 Process to confirm identity. 3.2 Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1 current residence, regardless of duration; and 3.2.2 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. 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. 3.3 Criteria or process to evaluate criminal history records checks for authorizing access. 3.4 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 3.5 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.	X						X			X	X					MC	**004-3 R3** Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include: R3.1 The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position. R3.2 The Responsible Entity shall update each personnel risk assessment at least every seven Years after the initial personnel risk assessment or for cause. R3.3 The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-3.

004-5 R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in CIP-004-5 Table R4 – Access Management Program. 4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1 Electronic access; 4.1.2 Unescorted physical access into a Physical Security Perimeter; and 4.1.3 Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. 4.2 Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. 4.3 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. 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.		X						X			X	X					MC		**003-3 R5.** Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information. R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities. R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information. **004-3 R4.** Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets. R4.1 The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained. **006-3 R1.** Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following: R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
004-5 R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in CIP-004-5 Table R5 – Access Revocation. 5.1 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.) 5.2 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. 5.3 For terminations actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.		X						X			X	X					MC		**003-3 R5.** Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information. R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities. R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information. **004-3 R4.** Access —The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets. R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
004-5 R5. 5.4 For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.		X									X						MC		R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.
004-5 R5. 5.5 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 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.		X									X						MC		**007-3 R5.** Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed. R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts. R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service. R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts. R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

Version 5	Applicability														Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
005-5 R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. 1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	X			X								X			MC	**005-3 R1**. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s). R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device. R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s). R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3. R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3. R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.
005-5 R1 1.2 All External Routable Connectivity must be through an identified Electronic Access Point (EAP).			X				X					X			MC	**005-3 R1.** R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
005-5 R1 1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	X						X						X		MC	**005-3 R2.** Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
005-5 R1 1.4 Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.		X				X						X			MC	**005-3 R2.** Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s). R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
005-5 R1 1.5 Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	X				X								X		MC	**005-3 R3**. Monitoring Electronic Access The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week. R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible. R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

005-5 R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, **where technically feasible**: 2.1 Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. 2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System. 2.3 Require multi-factor authentication for all Interactive Remote Access sessions.		X						X					X				MC		**005-3 R2.** Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified. R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services. R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s). R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible. R2.5. The required documentation shall, at least, identify and describe: R2.5.1. The processes for access request and authorization. R2.5.2. The authentication methods. R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. R2.5.4. The controls used to secure dial-up accessible connections.

Version 5	Applicability															Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
006-5 R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-5 Table R1 – Physical Security Plan. 1.1 Define operational or procedural controls to restrict physical access.	X						X	X			X				MC	**006-3 R1.** Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets. R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points. R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s). R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls. R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4. R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following: R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters. R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter. R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls. R1.8. Annual review of the physical security plan.
006-5 R1. 1.2 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. 1.3 **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.							X			X		X			MC	**006-3 R4.** Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. - Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
006-5 R1. 1.4 Monitor for unauthorized access through a physical access point into a Physical Security Perimeter. 1.5 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. 1.6 Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System. 1.7 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.	X						X			X		X			MC	**006-3 R5** Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: - Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. - Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. - Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. - Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
006-5 R1. 1.8 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.	X						X			X		X			MC	**006-3 R6**. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: - Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. - Video Recording: Electronic capture of video images of sufficient quality to determine identity. - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

006-5 R1. 1.9 Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.		X						X			X		X				MC		**006-3 R7.** Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.
006-5 R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in CIP-006-5 Table R2 – Visitor Control Program. 2.1 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. 2.2 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. 2.3 Retain visitor logs for at least ninety calendar days.		X						X			X		X				MC		**006-3 R1**. Physical Security Plan - The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets. R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points. R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s). R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls. R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4. R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following: R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters. R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter. R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls. R1.8. Annual review of the physical security plan.
006-5 R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in CIP-006-5 Table R3 – Maintenance and Testing Program. 3.1 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.		X						X				X			X		MC		**006-3 R8.** Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following: 8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years. 8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1. 8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

Version 5	Applicability														Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
007-5 R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R1 – Ports and Services. 1.1 **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 are open are deemed needed.	X						X			X	X	X			MC	**007-3 R2**. Ports and Services The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled. R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations. R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s). R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
007-5 R1. 1.2 Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	X				X										MC	
007-5 R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R2 – Security Patch Management. 2.1 A patch management process for tracking, evaluating, and installing cyber security 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. 2.2 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 2.3 For applicable patches identified in Part 2.2, within 35 calendar days of 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. 2.4 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.	X			X						X	X	X			MC	**007-3 R3.** Security Patch Management - The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s). R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades. R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
007-5 R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R3 – Malicious Code Prevention. 3.1 Deploy method(s) to deter, detect, or prevent malicious code. 3.2 Mitigate the threat of detected malicious code. 3.3 For those methods identified in Part 3.1 that use signatures or patterns, have a process for the updated of the signatures or patterns. The process must address testing and installing the signatures or patterns.	X			X						X	X	X			MC	**007-3 R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s). R4.1 The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure. R4.2 The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.
007-5 R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R4 – Security Event Monitoring. 4.1 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: 4.1.1 Detected successful login attempts; 4.1.2 Detected failed access attempts and failed login attempts; 4.1.3 Detected malicious code.	X			X						X	X	X			MC	**007-3 R6.** Security Status Monitoring - The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security. R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter. R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

007-5 R4. 4.2 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): 4.2.1 Detected malicious code from Part 4.1; and 4.2.2 Detected failure of Part 4.1 event logging.		X						X			X	X	X				MC		R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, **where technically feasible**, to support incident response as required in Standard CIP-008-3. R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days. R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.
007-5 R4. 4.3 **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.		X				X					X	X	X				MC		
007-5 R4. 4.4 Review and summarization of sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.		X									X		X				MC		
007-5 R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R5 – System Access Controls. 5.1 Have a method(s) to enforce authentication of interactive user access, where technically feasible.		X				X		X			X	X	X				MC		**007-3 R5.** Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. R5.1 The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed R5.1.1 The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5. R5.1.2 The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days. R5.1.3 The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4. R5.2 The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts. R5.2.1 The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service. R5.2.2 The Responsible Entity shall identify those individuals with access to shared accounts. R5.2.3 Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination). R5.3 At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible: R5.3.1 Each password shall be a minimum of six characters. R5.3.2 Each password shall consist of a combination of alpha, numeric, and "special" characters. R5.3.3 Each password shall be changed at least annually, or more frequently based on risk.
007 R5. 5.2 Identify and inventory all known enabled default or other generic account types, either by system, by grouped of systems, by location, or by system type(s).		X			X						X	X	X				MC		
007 R5. 5.3 Identify individuals who have authorized access to shared accounts.		X						X			X	X	X				MC		
007 R5. 5.4 Change known default passwords, per Cyber Asset capability 5.5 For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1 Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.		X			X						X	X	X				MC		
007 R5. 5.6 **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.		X						X			X	X	X				MC		
007 R5. 5.7 **Where technically feasible**, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.		X				X					X	X	X				MC		

Version 5	Applicability															Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
008-5 R1. 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-008-5 Table R1 – Cyber Security Incident Response Plan Specifications. 1.1 One or more processes to identify, classify, and respond to Cyber Security Incidents. 1.2 One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident. 1.3 The roles and responsibilities of Cyber Security Incident response groups or individuals. 1.4 Incident handling procedures for Cyber Security Incidents.	X			X											MC	**008-3 R1.** Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following: R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents. R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans. R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.
008-5 R2. 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-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. 2.1 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. 2.2 Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident 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. 2.3 Retain records related to Reportable Cyber Security Incidents.	X			X											MC	**008-3 R1**. Cyber Security Incident Response Plan - The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following: R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually. R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. **008-3 R2**. Cyber Security Incident Documentation - The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.
008-5 R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. 3.1 No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. 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. 3.2 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: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	X			X											MC	**008-3 R1.** R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

Version 5	Applicability															Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
009-5 R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-5 Table R1 – Recovery Plan Specifications. 1.1 Conditions for activation of the recovery plan(s). 1.2 Roles and responsibilities of responders. 1.3 One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	X			X						X	X				MC	**009-3 R1.** Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following: R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s). R1.2. Define the roles and responsibilities of responders. **009-3 R4**. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.
009-5 R1. 1.4 One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures..	X				X					X	X				New	
009-5 R1. 1.5 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.	X			X						X	X				New	
009-5 R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. 2.1 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. 2.2 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.	X				X					X	X				MC	**009-3 R2.** Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident. **009-3 R5.** Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.
009-5 R2. 2.3 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.	X														New	
009-5 R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication. 3.1 No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. 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. 3.2 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: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	X				X					X	X				MC	**009-3 R3.** Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

Version 5	Applicability															Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
010-1 R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R1 – Configuration Change Management. 1.1 Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied. 1.2 Authorize and document changes that deviate from the existing baseline configuration.	X			X						X	X	X			MC	**003-3 R6.** Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process. **005-3 R2**. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
010-1 R1. 1.3 For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	X		X							X	X	X			MC	**005-3 R5.** Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3. R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually. R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change. R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3. **007-3 R9.** Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.
010-1 R1. 1.4 For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	X			X						X	X	X			MC	**007-3 R1**. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware. R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation. R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment. R1.3. The Responsible Entity shall document test results.
010-1 R1. 1.5 **Where technically feasible**, for each change that deviates from the existing baseline configuration: 1.5.1. 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 1.5.2. 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.	X														MC	
010-1 R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R2 – Configuration Monitoring. 2.1 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.	X									X		X			MC	**003-3 R6.** Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.
010-1 R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R3– Vulnerability Assessments. 3.1 At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	X			X						X	X	X			MC	**005-3 R4.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

010-1 R3. 3.2 Where technically feasible, at least once every 36 calendar months: 3.2.1 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 3.2.2 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. 3.3 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. 3.4 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.		X															MC		R4.1. A document identifying the vulnerability assessment process; R4.2. A review to verify that only ports and services required for operations at these access points are enabled; R4.3. The discovery of all access points to the Electronic Security Perimeter; R4.4. A review of controls for default accounts, passwords, and network management community strings; R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan. **007-3 R1.** Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware. R1.1 The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

Version 5	Applicability															Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP		
011-1 R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-1 Table R1 – Information Protection. 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information. 1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	X			X						X	X				MC	**003-3 R4.** Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets. R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
011-1 R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. 2.1 Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media 2.2 Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	X			X						X	X	X			MC	**007-3 R7.** Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3. R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data. R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.