NERC CIP -1, -2 and -3: A Comparison

March 8, 2010

Prepared By:
Network & Security Technologies
161 North Middletown Road
Pearl River, NY 10965-2029
Phone: (845) 620-9500
http://www.netsectech.com

Executive Summary

Network & Security Technologies, Inc. ("N&ST") developed this tool to assist responsible entities updating their NERC CIP compliance programs from version one ("-1") to version two ("-2") of the standards. It provides a means to quickly identify differences between each version. N&ST consultants have used this to help clients prepare for the April 1, 2010 effective date of NERC CIP-002-2 through NERC CIP-009-2.

The tool comprises a line-by-line textual analysis of the -1 and -2 language. By focusing on the changes between versions, most responsible entities can modify their existing program without expending time and resources to respond to every CIP requirement.

This package also includes a comparison of the -2 and -3 language of the CIP standards. At the time of this writing, the latter awaits approval by FERC and no fixed implementation date for compliance has been set. While the -3 version of the Standards includes only a few material changes from the -2 version, responsible entities should not overlook them.

For best results, print the tables that make up the balance of this document in landscape mode on legal sized paper.

Table of Contents

About N&ST

Network & Security Technologies (N&ST) takes pride in helping our clients with their NERC CIP compliance needs. Our consultants follow a repeatable methodology to identify compliance gaps, implement remedial measures, and prepare for audits.

Our consultants:

- Have worked in the field of cyber security for the Bulk Electric System (BES) dating back to the NERC Urgent Action Standard 1200,
- Participate in NERC CIP Standards Drafting Team meetings,
- Know the current CIP-002 through CIP-009 -1, -2, and -3 requirements,
- Work with many BES companies across all aspects of the industry – transmission, generation, distribution, balancing and reliability coordinators,
- Understand all major energy management systems (EMS),
- Have hands-on experience with SCADA technologies including RTUs, relays, IEDs, and telecommunications devices,
- Understand routable protocols and data networks,
- Perform numerous gap analysis, compliance remediation, and audit preparation projects,
- Serve on NERC and regional entity CIP audit teams.

Our approach enables BES companies to have the information they need to protect against cyber security threats. Most importantly, we work quickly and efficiently so that responsible entities can meet their compliance deadlines and avoid negative audit findings. All N&ST consultants are full-time employees with many years of computer networking, cyber security, and electric utility industry experience. We carefully manage our projects to ensure complete customer satisfaction within the quoted timeframe and price.

Please contact us if you have any questions or need advice for a cyber security or network issue.

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
CIP–002 — Cyber Security — Critical Cyber Asset Identification	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	YES	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-assessment methodology to use to identify Critical Assets.	The word "its" was removed from v2
	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	NO	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	
	R1.2.	The risk-based assessment shall consider the following assets:	NO	R1.2.	The risk-based assessment shall consider the following assets:	
	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	NO	R1.2.1	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	
	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	NO	R1.2.2	Transmission substations that support the reliable operation of the Bulk Electric System.	
	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	NO	R1.2.3	Generation resources that support the reliable operation of the Bulk Electric System.	
	R1.2.4.	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	NO	R1.2.4	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	
	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	NO	R1.2.5	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	
	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	NO	R1.2.6	Special Protection Systems that support the reliable operation of the Bulk Electric System.	
	R1.2.7.	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	NO	R1.2.7	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	
	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.	NO	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.	
	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 interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	YES	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 interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	CIP-002 was updated to CIP-002-2
	R3.1.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	NO	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,	NO	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	
	R3.3.	The Cyber Asset is dial-up accessible.	NO	R3.3.	The Cyber Asset is dial-up accessible.	
	R4.	Annual Approval — A senior manager or delegate(s) shall approve annually 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 list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	YES	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.)	Changed "A senior manager" to "The senior manager" Adds requirement for annual approval of risk-based assessment methodology to existing requirement for annual approval of Critical Asset and Critical Cyber Asset lists

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
CIP–003 — Cyber Security — Security Management Controls	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:	NO	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 through CIP-009, including provision for emergency situations.	YES	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.	"CIP-002 through CIP-009" changed to "CIP-002-2 through CIP-009-2"
	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	NO	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	
	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	NO	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	
	R2.	Leadership - The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.	YES	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-002-2 through CIP-009-2.	Reworded to clarify the Responsible Entity must assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2 "CIP-002 through CIP-009" changed to "CIP-002-2 through CIP-009-2"
	R2.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	YES	R2.1.	The senior manager shall be identified by name, title, and date of designation.	Drops requirement to include this individual's business phone and business address with identifying records
	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	NO	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	
			YES	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, 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.	
	R2.3.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	NO	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	
	R3.	Exceptions - Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	NO	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	
	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	NO	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	
	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	YES	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	Removed "or a statement accepting risk."
	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	NO	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	
	R4.	Information Protection - The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	NO	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, 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.	YES	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-002-2, 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.	CIP-002 was updated to CIP-002-2

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	NO	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	
	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	NO	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	
	R5.	Access Control - The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	NO	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	
	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	NO	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	
	R5.1.1.	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	YES	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	Drops requirement to include this individual's business phone with identifying records
	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	NO	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	
	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.	NO	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.	NO	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	
	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.	NO	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.	
	R1.	Awareness - The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access 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:	YES	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:	Reworded to clarify the Responsible Entity must establish, document, and implement an awareness program
		o Direct communications (e.g., emails, memos, computer based training, etc.);	NO		Direct communications (e.g. emails, memos, computer based training, etc.);	
		o Indirect communications (e.g., posters, intranet, brochures, etc.);	NO		Indirect communications (e.g. posters, intranet, brochures, etc.);	
		o Management support and reinforcement (e.g., presentations, meetings, etc.).	NO		Management support and reinforcement (e.g., presentations, meetings, etc.).	
	R2.	Training - The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	YES	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.	Reworded to clarify the Responsible Entity must establish, document, and implement a training program Reworded to indicate the Responsible Entity must review the program annually at a minimum and update it as necessary
	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	YES	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.	Requires training of personnel prior to their being granted such access "…except in specified circumstances such as an emergency."

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
CIP–004 — Cyber Security — Personnel and Training	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	YES	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	Updated "CIP-004" to "CIP-004-2"
	R2.2.1.	The proper use of Critical Cyber Assets;	NO	R2.2.1.	The proper use of Critical Cyber Assets;	
	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	NO	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	
	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	NO	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 thereto following a Cyber Security Incident.	NO	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	
	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	NO	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	
	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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	YES	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:	Clarifies that requirements apply to those with access to Critical Cyber Assets. Requires assessments of personnel prior to their being granted such access "…except in specified circumstances such as an emergency."
	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.	NO	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.	NO	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.	YES	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-004-2.	Updated "CIP-004" to "CIP-004-2"
	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.	NO	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.	NO	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.	
	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.	NO	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.	
	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).	NO	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).	

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
CIP–005 — Cyber Security — Electronic Security Perimeter(s)	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).	NO	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).	
	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.	NO	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).	NO	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.	YES	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-005-2.	Updated "CIP-005" to "CIP-005-2"
	R1.5.	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	YES	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-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	Reworded to: “Cyber Assets used in the access control *and/o*r monitoring of the Electronic Security Perimeter(s)…” Updated "CIP-003" to "CIP-003-2" Updated "CIP-004" to "CIP-004-2" Updated "CIP-005" to "CIP-005-2" Updated "CIP-006" to "CIP-006-2" Updated "CIP-007" to "CIP-007-2" Updated "CIP-008" to "CIP-008-2" Updated "CIP-009" to "CIP-009-2"
	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.	NO	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.	
	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).	NO	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.	NO	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.	NO	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 maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	YES	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	Reworded to clarify the Responsible Entity must implement and maintain a procedure for securing dial-up access
	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.	NO	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:	NO	R2.5.	The required documentation shall, at least, identify and describe:	
	R2.5.1.	The processes for access request and authorization.	NO	R2.5.1.	The processes for access request and authorization.	
	R2.5.2.	The authentication methods.	NO	R2.5.2.	The authentication methods.	

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.	YES	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.	Updated "CIP-004" to "CIP-004-2"
	R2.5.4.	The controls used to secure dial-up accessible connections.	NO	R2.5.4.	The controls used to secure dial-up accessible connections.	
	R2.6.	Appropriate Use Banner - Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	NO	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	
	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.	NO	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.	NO	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.	NO	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.	
	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:	NO	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:	
	R4.1.	A document identifying the vulnerability assessment process:	NO	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:	NO	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:	NO	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; and,	YES	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	The work "and" was removed
	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.	NO	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.	
	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.	YES	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.	Updated "CIP-005" to "CIP-005-2"
	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP- 005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.	YES	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.	Updated "CIP-005" to "CIP-005-2"
	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.	NO	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.	YES	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-008-2.	Updated "CIP-008" to "CIP-008-2"
	R1.	Physical Security Plan - The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	YES	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:	Reworded to clarify the Responsible Entity must document, implement, and maintain a physical security plan. Clarified that the Physical Security Plan shall be approved by *the* senior manager.

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
	R1.1.	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also 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 the Critical Cyber Assets.	YES	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.	Reworded to clarify that Cyber Assets within an ESP shall reside in a Physical Security Perimeter, rather than the establishment of processes.
	R1.2.	Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.	YES	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	Reworded to clarify that the identification of all access points through the Physical Security Perimeter is to be measured, rather than the establishment of processes.
	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	NO	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	
	R1.4.	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	YES	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.	Reworded to clarify that the use of physical access controls is to be measured, rather than the establishment of processes.
	R1.5.	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	YES	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	Reworded to clarify that the review of access authorization requests and revocations is to be measured, rather than the establishment of processes.
	R1.6.	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	YES	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	Modified to require, "Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access."
	R1.7.	Process for updating the physical security plan within ninety calendar days 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.	YES	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.	Modified to require "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" from ninety days.
	R1.8.	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	YES			Requirement moved to R2.2
	R1.9.	Process for ensuring that the physical security plan is reviewed at least annually.	YES	R1.8.	Annual review of the physical security plan.	Reworded to clarify that the annual review of the physical security plan is to be measured, rather than the establishment of processes.
			YES	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	
			YES	R2.1.	Be protected from unauthorized physical access.	
			YES	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	Formerly R1.8
CIP-006 — Cyber Security — Physical Security of Critical			YES	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
Cyber Assets	R2.	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:	YES	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:	Moved from R2. to R4. Content remains the same
	R2.1.	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.	YES		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.	Changed from sub-requirement to bullet point
	R2.2.	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.	YES		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.	Changed from sub-requirement to bullet point
	R2.3.	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	YES		Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	Changed from sub-requirement to bullet point
	R2.4.	Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	YES		Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	Changed from sub-requirement to bullet point
	R3.	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. One or more of the following monitoring methods shall be used:	YES	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-008-2. One or more of the following monitoring methods shall be used:	Moved from R3. to R5. Updated "CIP-008" to "CIP-008-2"
	R3.1.	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.	YES		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.	Changed from sub-requirement to bullet point
	R3.2.	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.	YES		Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	Changed from sub-requirement to bullet point
	R4.	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 more of the following logging methods or their equivalent:	YES	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:	Moved from R4. to R6.
	R4.1.	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	YES		Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.	Changed from sub-requirement to bullet point
	R4.2.	Video Recording: Electronic capture of video images of sufficient quality to determine identity.	YES		Video Recording: Electronic capture of video images of sufficient quality to determine identity.	Changed from sub-requirement to bullet point
	R4.3.	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 R2.3.	YES		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.	Changed from sub-requirement to bullet point Updated "Requirement R2.3" to "Requirement R4."
	R5.	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.	YES	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-008-2.	Moved from R5. to R7. Updated "CIP-008" to "CIP-008-2"
	R6.	Maintenance and Testing - The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	YES	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:	Moved from R6. to R8. Updated "Requirements R2, R3, and R4" to "Requirements R4, R5, and R6"
	R6.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	YES	R8.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	Moved from R6.1. to R8.1.
	R6.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	YES	R8.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	Moved from R6.2. to R8.2. Updated "Requirement R6.1." to "Requirement R8.1."

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
	R6.3.	Retention of outage records regarding access controls, logging, and monitoring for minimum of one calendar year.	YES	R8.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	Moved from R6.3. to R8.3.
	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, 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.	YES	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-007-2, 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.	Updated "CIP-007" to "CIP-007-2"
	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.	NO	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.	NO	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.	NO	R1.3.	The Responsible Entity shall document test results.	
	R2.	Ports and Services - The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	YES	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.	Reworded to clarify the Responsible Entity must 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.	NO	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).	NO	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 or an acceptance of risk.	YES	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.	Removed "or an acceptance of risk."
	R3.	Security Patch Management - The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document 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).	YES	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 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).	Reworded to clarify the Responsible Entity must establish, document and implement a security patch management program Updated "CIP-003" to "CIP-003-2"
	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.	NO	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 or an acceptance of risk.	YES	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.	Removed "or an acceptance of risk."
	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).	NO	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 or an acceptance of risk.	YES	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.	Removed "or an acceptance of risk."

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
CIP–007 — Cyber Security — Systems Security Management	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.	NO	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.	
	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.	NO	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.	NO	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 Requirement R5.	YES	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.	Updated "CIP-003" to "CIP-003-2"
	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.	NO	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 Requirement R5 and Standard CIP-004 Requirement R4.	YES	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.	Updated "CIP-003" to "CIP-003-2" Updated "CIP-004" to "CIP-004-2"
	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.	NO	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.	NO	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.	NO	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).	NO	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:	NO	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.	NO	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.	NO	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.	NO	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	
	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.	NO	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.	NO	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.	NO	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	
	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.	YES	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-008-2.	Updated "CIP-008" to "CIP-008-2"

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	NO	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.	NO	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	
	R7.	Disposal or Redeployment - The Responsible Entity shall establish 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.	YES	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-005-2.	Reworded to clarify the Responsible Entity must establish and implement Disposal or Redeployment methods, processes, and procedures. Updated "CIP-005" to "CIP-005-2"
	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.	NO	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.	NO	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.	
	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	NO	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	
	R8.	Cyber Vulnerability Assessment - The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	NO	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	
	R8.1.	A document identifying the vulnerability assessment process;	NO	R8.1.	A document identifying the vulnerability assessment process;	
	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	NO	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	
	R8.3.	A review of controls for default accounts; and,	NO	R8.3.	A review of controls for default accounts; and,	
	R8.4.	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.	NO	R8.4.	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.	
	R9.	Documentation Review and Maintenance - The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	YES	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	Modified to require updates to documentation within thirty calendar days of the completion of changes resulting from modifications to systems or controls from ninety days.
CIP–008 — Cyber Security — Incident Reporting and Response Planning	R1.	Cyber Security Incident Response Plan - The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	YES	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:	Modified to require the Responsible Entity to implement the plan it has developed and maintained in response to Cyber Security Incidents
	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	NO	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	
	R1.2.	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	YES	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	Rewritten to clarify that roles and responsibilities applies to Cyber Security Incident Response Teams. Rewritten to clarify that incident handling procedures apply to Cyber Security incidents.
	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.	YES	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.	Changed "ES ISAC" to "ES-ISAC"
	R1.4.	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	YES	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	Modified to require that the Incident Response Plan must be updated within thirty calendar days of any changes from ninety calendar days.

Standard	v1 Req Number	v1 Requirement	Did the requirement change?	v2 Req Number	v2 Requirement	Change Discussion
	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	NO	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 incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	YES	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. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.	Adds the statement, “Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.”
	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.	NO	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.	
CIP–009 — Cyber Security — Recovery Plans for Critical Cyber Assets	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:	NO	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).	NO	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.	NO	R1.2.	Define the roles and responsibilities of responders.	
	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.	NO	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.	
	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 ninety calendar days of the change.	YES	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.	Modified to require that changes to the Recovery Plan must be “…communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.” from ninety days.
	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.	NO	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.	
	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.	NO	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.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
CIP–002 — Cyber Security — Critical Cyber Asset Identification	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-assessment methodology to use to identify Critical Assets.	YES	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	"Its" was added to add more specificity to the Critical Assets identified.
	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	NO	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	
	R1.2.	The risk-based assessment shall consider the following assets:	NO	R1.2.	The risk-based assessment shall consider the following assets:	
	R1.2.1	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	NO	R1.2.1	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	
	R1.2.2	Transmission substations that support the reliable operation of the Bulk Electric System.	NO	R1.2.2	Transmission substations that support the reliable operation of the Bulk Electric System.	
	R1.2.3	Generation resources that support the reliable operation of the Bulk Electric System.	NO	R1.2.3	Generation resources that support the reliable operation of the Bulk Electric System.	
	R1.2.4	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	NO	R1.2.4	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	
	R1.2.5	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	NO	R1.2.5	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	
	R1.2.6	Special Protection Systems that support the reliable operation of the Bulk Electric System.	NO	R1.2.6	Special Protection Systems that support the reliable operation of the Bulk Electric System.	
	R1.2.7	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	NO	R1.2.7	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	
	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.	NO	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.	
	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 interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	YES	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:	Changed standards reference from v2 to v3.
	R3.1.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	NO	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,	NO	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	
	R3.3.	The Cyber Asset is dial-up accessible.	NO	R3.3.	The Cyber Asset is dial-up accessible.	
	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.)	NO	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.)	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
CIP–003 — Cyber Security — Security Management Controls	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:	NO	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-002-2 through CIP-009-2, including provision for emergency situations.	YES	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.	Changed standards reference from v2 to v3.
	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	NO	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	
	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	NO	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	
	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-002-2 through CIP-009-2.	YES	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.	Changed standards reference from v2 to v3.
	R2.1.	The senior manager shall be identified by name, title, and date of designation.	NO	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.	NO	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	
	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, 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.	YES	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.	Changed standards reference from v2 to v3.
	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	NO	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	
	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	NO	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	
	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	NO	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	
	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	NO	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	
	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	NO	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	
	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	NO	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-002-2, 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.	YES	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.	Changed standards reference from v2 to v3.
	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	NO	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	
	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	NO	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	NO	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	
	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	NO	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	
	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	NO	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	
	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	NO	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	
	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.	NO	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.	NO	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	
	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.	YES	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.	"vendor related" in v2 is changed to "vendor-related" in v3.
	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:	NO	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.);	YES		Direct communications (e.g., emails, memos, computer based training, etc.);	added a comma after "e.g."
		Indirect communications (e.g. posters, intranet, brochures, etc.);	YES		Indirect communications (e.g., posters, intranet, brochures, etc.);	added a comma after "e.g."
		Management support and reinforcement (e.g., presentations, meetings, etc.).	NO		Management support and reinforcement (e.g., presentations, meetings, etc.).	
	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.	NO	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.	NO	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-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	YES	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:	Changed standards reference from v2 to v3.
	R2.2.1.	The proper use of Critical Cyber Assets;	NO	R2.2.1.	The proper use of Critical Cyber Assets;	
	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	NO	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	
	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	NO	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 thereto following a Cyber Security Incident.	NO	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
CIP–004 — Cyber Security — Personnel and Training	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	NO	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	
	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:	NO	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.	YES	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.	"seven year" in v2 changed to "seven-year" in v3
	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.	NO	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-004-2.	YES	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.	Changed standards reference from v2 to v3.
	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.	NO	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.	NO	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.	
	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.	NO	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.	
	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).	NO	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).	
	R1.1.	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).	NO	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).	
	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.	NO	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.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
CIP–005 — Cyber Security — Electronic Security Perimeter(s)	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).	NO	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-005-2.	YES	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.	Changed standards reference from v2 to v3.
	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-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	YES	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.	Changed standards reference from v2 to v3.
	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.	NO	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.	
	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).	NO	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.	NO	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.	NO	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).	NO	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.	NO	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:	NO	R2.5.	The required documentation shall, at least, identify and describe:	
	R2.5.1.	The processes for access request and authorization.	NO	R2.5.1.	The processes for access request and authorization.	
	R2.5.2.	The authentication methods.	NO	R2.5.2.	The authentication methods.	
	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.	YES	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.	Changed standards reference from v2 to v3.
	R2.5.4.	The controls used to secure dial-up accessible connections.	NO	R2.5.4.	The controls used to secure dial-up accessible connections.	
	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	NO	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	
	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.	NO	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.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
	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.	NO	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.	NO	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.	
	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:	NO	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:	
	R4.1.	A document identifying the vulnerability assessment process;	NO	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;	NO	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;	NO	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;	NO	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.	NO	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.	
	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.	YES	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.	Changed standards reference from v2 to v3.
	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.	YES	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.	Changed standards reference from v2 to v3.
	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.	NO	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-008-2.	YES	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.	Changed standards reference from v2 to v3.
	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:	NO	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.	NO	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.	NO	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).	NO	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.	NO	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-004-2 Requirement R4.	YES	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	Changed standards reference from v2 to v3.

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
CIP-006 — Cyber Security — Physical Security of Critical Cyber Assets	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	YES	R1.6.	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	Established a "Visitor Control Program" rather than simply requiring continuous access.
			YES	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.	Must document a vistor entering and leaving a PSP
			YES	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter.	Must provide continuous escort
	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.	NO	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.	NO	R1.8.	Annual review of the physical security plan.	
	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	NO	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	
	R2.1.	Be protected from unauthorized physical access.	NO	R2.1.	Be protected from unauthorized physical access.	
	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	YES	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP- 004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP- 006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	Changed standards reference from v2 to v3.
	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	NO	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	
	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:	NO	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.	NO		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.	NO		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.	
		Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	NO		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.	NO		Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	
	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-008-2. One or more of the following monitoring methods shall be used:	YES	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:	Changed standards reference from v2 to v3.
		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.	NO		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.	NO		Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
	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:	NO	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.	NO		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.	NO		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.	NO		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.	
	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-008-2.	YES	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.	Changed standards reference from v2 to v3.
	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:	NO	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:	
	R8.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	NO	R8.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	
	R8.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	NO	R8.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	
	R8.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	NO	R8.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	
	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-007-2, 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.	YES	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.	Changed standards reference from v2 to v3.
	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.	NO	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.	NO	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.	NO	R1.3.	The Responsible Entity shall document test results.	
	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.	NO	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.	NO	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).	NO	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.	NO	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.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
CIP–007 — Cyber Security — Systems Security Management	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 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).	YES	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).	Changed standards reference from v2 to v3.
	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.	NO	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.	NO	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.	
	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).	NO	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.	NO	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.	NO	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.	
	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.	NO	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.	NO	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-003-2 Requirement R5.	YES	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.	Changed standards reference from v2 to v3.
	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.	NO	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-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.	YES	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.	Changed standards reference from v2 to v3.
	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.	NO	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.	NO	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.	NO	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
	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).	NO	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:	NO	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.	NO	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.	NO	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.	NO	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	
	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.	NO	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.	NO	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.	NO	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	
	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-008-2.	YES	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.	Changed standards reference from v2 to v3.
	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	NO	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.	NO	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	
	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-005-2.	YES	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.	Changed standards reference from v2 to v3.
	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.	NO	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.	NO	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.	
	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	NO	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	
	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	NO	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	
	R8.1.	A document identifying the vulnerability assessment process;	NO	R8.1.	A document identifying the vulnerability assessment process;	
	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	NO	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	
	R8.3.	A review of controls for default accounts; and,	NO	R8.3.	A review of controls for default accounts; and,	
	R8.4.	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.	NO	R8.4.	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.	

Standard	v2 Req Number	v2 Requirement	Did the requirement change?	v3 Req Number	v3 Requirement	Change Discussion
	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	YES	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.	Changed standards reference from v2 to v3.
CIP–008 — Cyber Security — Incident Reporting and Response Planning	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:	NO	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.	NO	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.	NO	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.	NO	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.	
	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	NO	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	
	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	NO	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. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.	YES	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.	Removed "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test."
	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.	NO	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.	
CIP–009 — Cyber Security — Recovery Plans for Critical Cyber Assets	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:	NO	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).	NO	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.	NO	R1.2.	Define the roles and responsibilities of responders.	
	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.	NO	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.	
	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.	NO	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.	
	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.	NO	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.	
	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.	NO	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.	