NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 (CIP-002-5, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-6 R1	No change.
CIP-003-5 R1.1	CIP-003-6 R1.1	No change.
CIP-003-5 R1.2	CIP-003-6 R1.2	No change.
CIP-003-5 R1.3	CIP-003-6 R1.3	No change.
CIP-003-5 R1.4	CIP-003-6 R1.4	No change.
CIP-003-5 R1.5	CIP-003-6 R1.5	No change.
CIP-003-5 R1.6	CIP-003-6 R1.6	No change.
CIP-003-5 R1.7	CIP-003-6 R1.7	No change.
CIP-003-5 R1.8	CIP-003-6 R1.8	No change.
CIP-003-5 R1.9	CIP-003-6 R1.9	No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2	CIP-003-6 R2, CIP-003-6, R2.1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. The main requirement was modified to follow a similar structure to parent Requirements of those requirement parts in the table format. The CIP Senior Manager review and approval at least once every 15 months was mapped to CIP-003-6 R2.1.
CIP-003-5 R2.1	CIP-003-6 R2.6	The security awareness requirement part was mapped to Part 2.6 to reinforce cyber security practices at least quarterly, while addressing Parts 2.2 through 2.5 once every 15 calendar months. This added objective criteria to security awareness, while not to the rigor of Medium and High BES Cyber Systems.
CIP-003-5 R2.2	CIP-003-6 R2.2	Expanding the physical security controls, Part 2.2 addresses operational or procedural control(s) to restrict physical access.
NEW	CIP-003-6 R2.3	Expanding the physical security controls, Part 2.3 requires implementation of processes to include Parts 2.3.1 and 2.3.2 for low impact BES Cyber Systems at Control Centers.
NEW	CIP-003-6 R2.3.1	Expanding the physical security controls, Part 2.3.1 addresses escorted access of visitors at Control Centers.
NEW	CIP-003-6 R2.3.2	Expanding the physical security controls, Part 2.3.2 addresses monitored physical access point(s) at Control Centers with external routable protocol paths.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.3	CIP-003-6 R2.4	The electronic access controls were added as Part 2.4. The documented process(es) collectively must include Parts 2.4.1 through 2.4.3.
NEW	CIP-003-6 R2.4.1	Expanding the electronic access controls, Part 2.4.1 addresses all external routable protocol paths, if any, as needing to be through one or more identified access point(s).
NEW	CIP-003-6 R2.4.2	Expanding the electronic access controls, Part 2.4.2 addresses requiring inbound and outbound access permissions for each identified access point, including the reason for granting access, and deny all other access by default.
NEW	CIP-003-6 R2.4.3	Expanding the electronic access controls, Part 2.4.3 addresses authentication when establishing Dial-Up Connectivity, per Cyber Asset capability.
CIP-003-5 R2.4	CIP-003-6 R2.5	The incident response to a Cyber Security Incident requirement part remains in Part 2.5. The documented response plan(s) collectively must include Parts 2.5.1 through 2.5.6.
NEW	CIP-003-6 R2.5.1	Expanding the incident response controls, Part 2.5.1 address the identification, classification, and response to Cyber Security Incidents.
NEW	CIP-003-6 R2.5.2	Expanding the incident response controls, Part 2.5.2 addresses whether an identified Cyber Security Incident is reportable.
NEW	CIP-003-6 R2.5.3	Expanding the incident response controls, Part 2.5.3 addresses the notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-003-6 R2.5.4	Expanding the incident response controls, Part 2.5.4 addresses the roles and responsibilities of Cyber Security Incident response groups or individuals.
NEW	CIP-003-6 R2.5.5	Expanding the incident response controls, Part 2.5.5 addresses the incident handling procedures for Cyber Security Incidents.
NEW	CIP-003-6 R2.5.6	Expanding the incident response controls, Part 2.5.6 addresses the testing of the plan(s) at least once per 36 calendar months.
CIP-003-5 R3	CIP-003-6 R3	No change.
CIP-003-5 R4	CIP-003-6 R4	To respond to the FERC Order 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-6 R1	No change.
CIP-004-5.1 R1.1	CIP-004-6 R1.1	No change.
CIP-004-5.1 R2	CIP-004-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. The SDT has also revised the requirement to allow Responsible Entities the flexibility to have one or more cyber security training programs, as the existing CIP-004-5 R2 had Responsible Entities shall implement "a cyber security training program(s)." That modification was made for clarity and consistency across the standards.
CIP-004-5.1 R2.1	CIP-004-6 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-6 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-6 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-6 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-6 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004-6 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-6 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-6 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-6 R2.1.8	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.1.9	CIP-004-6 R2.1.9	To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Registered Entity's cyber security training program. The training must address cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with Transient Cyber Assets and Removable Media.
CIP-004-5.1 R2.2	CIP-004-6 R2.2	No change.
CIP-004-5.1 R2.3	CIP-004-6 R2.3	No change.
CIP-004-5.1 R3	CIP-004-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-004-5.1 R3.1	CIP-004-6 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-6 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-6 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-6 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-6 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-6 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-6 R3.5	No change.
CIP-004-5.1 R4	CIP-004-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-004-5.1 R4.1	CIP-004-6 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-6 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-6 R4.1.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R4.1.3	CIP-004-6 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-6 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004-6 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-6 R4.4	No change.
CIP-004-5.1 R5	CIP-004-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R5.1	CIP-004-6 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-6 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-6 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-6 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-6 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R1.1	CIP-007-6 R1.1	No change.
CIP-007-5 R1.2	CIP-007-6 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection again the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R2.1	CIP-007-6 R2.1	No change.
CIP-007-5 R2.2	CIP-007-6 R2.2	No change.
CIP-007-5 R2.3	CIP-007-6 R2.3	No change.
CIP-007-5 R2.4	CIP-007-6 R2.4	No change.
CIP-007-5 R3	CIP-007-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R3.1	CIP-007-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3.2	CIP-007-6 R3.2	No change.
CIP-007-5 R3.3	CIP-007-6 R3.3	No change.
CIP-007-5 R4	CIP-007-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-007-5 R4.1	CIP-007-6 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-6 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-6 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-6 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-6 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-6 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-6 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-6 R4.3	No change.
CIP-007-5 R4.4	CIP-007-6 R4.4	No change.
CIP-007-5 R5	CIP-007-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R4	CIP-007-6 R4	No change.
CIP-007-5 R5	CIP-007-6 R5	No change.
CIP-007-5 R5.1	CIP-007-6 R5.1	No change.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5.4	CIP-007-6 R5.4	No change.
CIP-007-5 R5.5	CIP-007-6 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-6 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-6 R5.5.2	No change.
CIP-007-5 R6	CIP-007-6 R6	No change.
CIP-007-5 R7	CIP-007-6 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R1.1	CIP-010-2 R1.1	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-2 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-2 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-2 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-2 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-2 R1.5.2	No change.
CIP-010-1 R2	CIP-010-2 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R2.1	CIP-010-2 R2.1	No change.
CIP-010-1 R3	CIP-010-2 R3	No change.
CIP-010-1 R3.1	CIP-010-2 R3.1	No change.
CIP-010-1 R3.2	CIP-010-2 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-2 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-2 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-2 R3.3	No change.
CIP-010-1 R3.4	CIP-010-2 R3.4	No change.
NEW	CIP-010-2 R4	To respond to the FERC Order No. 791 directive to address transient devices, new Requirement R4 follows the table format to ensure Registered Entities implemented one or more documented process(es) that collectively include each of the applicable parts in CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection. All of the new Requirement Parts under Requirement R4 are in response to this directive.
NEW	CIP-010-2 R4.1	Part 4.1 ensures Responsible Entities authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. The authorization shall include the Requirement Parts 4.1.1 through 4.1.4.
NEW	CIP-010-2 R4.1.1	Authorization shall include users, individually or by group/role.
NEW	CIP-010-2 R4.1.2	Authorization shall include locations, individually or by group/role.
NEW	CIP-010-2 R4.1.3	Authorization shall include defined acceptable use.
NEW	CIP-010-2 R4.1.4	Authorization shall include operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-2 R4.2	Part 4.2 ensures Responsible Entities use method(s) to deter, detect, or prevent malicious code introduction on Transient Cyber Assets (per Cyber Asset capability).
	CIP-010-2 R4.3	Part 4.3 ensures Responsible Entities use method(s) to detect malicious code on Removable Media prior to use on applicable systems.
NEW	CIP-010-2 R4.4	Part 4.4 ensures Responsible Entities mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.
NEW	CIP-010-2 R4.5	Part 4.5 ensures Responsible Entities update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.
NEW	CIP-010-2 R4.6	Part 4.6 ensures Responsible Entities evaluate Transient Cyber Assets prior to use for modifications that deviate from Part 4.1.4.
NEW	CIP-010-2 R4.7	Part 4.7 ensures Responsible Entities evaluate Transient Cyber Assets periodically to ensure security patches are up-to-date.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-2 R1.1	No change.
CIP-011-1 R1.2	CIP-011-2 R1.2	No change.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R2	CIP-011-2 R2	No change.
CIP-011-1 R2.1	CIP-011-2 R2.1	No change.
CIP-011-1 R2.2	CIP-011-2 R2.2	No change.