

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-~~67~~, CIP-004-~~67~~, CIP-006-6, CIP-007-~~67~~, CIP-009-6, CIP-010-~~23~~, and CIP-011-~~2-3~~ (CIP-002-5-1, 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- 67 R1	To incorporate a policy or policies for low impact BES Cyber Systems, the main requirement language was modified. “For its high impact and medium impact BES Cyber Systems” was struck from the language as new requirement parts were created. See below for part 1.1 and part 1.2 to see the change justification.
NEW	CIP-003- 67 R1.1	“For its high impact and medium impact BES Cyber Systems” was added as a qualifier to the sub-parts below.
CIP-003-5 R1.1	CIP-003- 67 R1.1.1	Requirement parts for 1.1 through 1.9 have become 1.1.1 through 1.1.9 with the clarifier added above in part 1.1 of CIP-003- 67 .
CIP-003-5 R1.2	CIP-003- 67 R1.1.2	No change.
CIP-003-5 R1.3	CIP-003- 67 R1.1.3	No change.
CIP-003-5 R1.4	CIP-003- 67 R1.1.4	No change.
CIP-003-5 R1.5	CIP-003- 67 R1.1.5	No change.
CIP-003-5 R1.6	CIP-003- 67 R1.1.6	No change.
CIP-003-5 R1.7	CIP-003- 67 R1.1.7	No change.
CIP-003-5 R1.8	CIP-003- 67 R1.1.8	No change.
CIP-003-5 R1.9	CIP-003- 67 R1.1.9	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
NEW	CIP-003- 67 R1.2	“For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:” was added as a qualifier to the sub-parts below.
CIP-003-5 R2	CIP-003- 67 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. Furthermore, as the SDT modified its approach of using Attachment 1 instead of the table approach, it modified Requirement R2 to “implement one or more document cyber security plan(s) that include the applicable elements in Attachment 1.”
CIP-003-5 R2.1	CIP-003- 67 R1.2.1	The security awareness requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003- 67 , Requirement R1, Part 1.2.1.
CIP-003-5 R2.2	CIP-003- 67 , R1.2.2	The physical security controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003- 67 , Requirement R1, Part 1.2.2.

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- 67 R1.2.3	The electronic access controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003- 67 , Requirement R1, Part 1.2.3. Furthermore, the SDT modified the “external routable protocol connections” as a new definition is being proposed by the SDT for “Low Impact External Routable Connectivity.”
CIP-003-5 R2.4	CIP-003- 67 R1.2.4	The incident response to a Cyber Security Incident requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003- 67 , Requirement R1, Part 1.2.4.
NEW	CIP-003- 67 , Attachment 1	CIP-003- 67 Attachment 1 lists the elements required for low impact asset cyber security plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the lack of objective criteria for Low Impact assets protections.
CIP-003-5 R3	CIP-003- 67 R3	No change.
CIP-003-5 R4	CIP-003- 67 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.

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- 67 R1	No change.
CIP-004-5.1 R1.1	CIP-004- 67 R1.1	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	CIP-004- 6-7 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- 6-7 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004- 6-7 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004- 6-7 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004- 6-7 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004- 6-7 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004- 6-7 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004- 6-7 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004- 6-7 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004- 6-7 R2.1.8	No change.
CIP-004-5.1 R2.1.9	CIP-004- 6-7 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- 6-7 R2.2	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 R2.3	CIP-004- 6-7 R2.3	No change.
CIP-004-5.1 R3	CIP-004- 6-7 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- 6-7 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004- 6-7 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004- 6-7 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004- 6-7 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004- 6-7 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004- 6-7 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004- 6-7 R3.5	No change.
CIP-004-5.1 R4	CIP-004- 6-7 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- 6-7 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004- 6-7 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004- 6-7 R4.1.2	No change.
CIP-004-5.1 R4.1.3	CIP-004- 6-7 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004- 6-7 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004- 6-7 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004- 6-7 R4.4	No change.
CIP-004-5.1 R5	CIP-004- 6-7 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.

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 R5.1	CIP-004- 6-7 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004- 6-7 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004- 6-7 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004- 6-7 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004- 6-7 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.
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.

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
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 <u>7</u> 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 <u>7</u> R1.1	No change.
CIP-007-5 R1.2	CIP-007- 6 <u>7</u> 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 against 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 <u>7</u> 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 <u>7</u> R2.1	No change.
CIP-007-5 R2.2	CIP-007- 6 <u>7</u> R2.2	No change.
CIP-007-5 R2.3	CIP-007- 6 <u>7</u> R2.3	No change.
CIP-007-5 R2.4	CIP-007- 6 <u>7</u> R2.4	No change.
CIP-007-5 R3	CIP-007- 6 <u>7</u> 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 <u>7</u> 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- 6-7 R3.2	No change.
CIP-007-5 R3.3	CIP-007- 6-7 R3.3	No change.
CIP-007-5 R4	CIP-007- 6-7 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- 6-7 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007- 6-7 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007- 6-7 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007- 6-7 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007- 6-7 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007- 6-7 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007- 6-7 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007- 6-7 R4.3	No change.
CIP-007-5 R4.4	CIP-007- 6-7 R4.4	No change.
CIP-007-5 R5	CIP-007- 6-7 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- 6-7 R5.2	No change.
CIP-007-5 R5.3	CIP-007- 6-7 R5.3	No change.
CIP-007-5 R4	CIP-007- 6-7 R4	No change.
CIP-007-5 R5	CIP-007- 6-7 R5	No change.
CIP-007-5 R5.1	CIP-007- 6-7 R5.1	No change.
CIP-007-5 R5.2	CIP-007- 6-7 R5.2	No change.
CIP-007-5 R5.3	CIP-007- 6-7 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 <u>7</u> R5.4	No change.
CIP-007-5 R5.5	CIP-007- 6 <u>7</u> R5.5	No change.
CIP-007-5 R5.5.1	CIP-007- 6 <u>7</u> R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007- 6 <u>7</u> R5.5.2	No change.
CIP-007-5 R6	CIP-007- 6 <u>7</u> R6	No change.
CIP-007-5 R7	CIP-007- 6 <u>7</u> 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 <u>3</u> 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 <u>3</u> R1.1	No change.
CIP-010-1 R1.2	CIP-010- 2 <u>3</u> R1.2	No change.
CIP-010-1 R1.3	CIP-010- 2 <u>3</u> R1.3	No change.
CIP-010-1 R1.4	CIP-010- 2 <u>3</u> R1.4	No change.
CIP-010-1 R1.5	CIP-010- 2 <u>3</u> R1.5	No change.
CIP-010-1 R1.2	CIP-010- 2 <u>3</u> R1.2	No change.
CIP-010-1 R1.3	CIP-010- 2 <u>3</u> R1.3	No change.
CIP-010-1 R1.4	CIP-010- 2 <u>3</u> R1.4	No change.
CIP-010-1 R1.4.1	CIP-010- 2 <u>3</u> R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010- 2 <u>3</u> R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010- 2 <u>3</u> R1.4.3	No change.
CIP-010-1 R1.5	CIP-010- 2 <u>3</u> R1.5	No change.
CIP-010-1 R1.5.1	CIP-010- 2 <u>3</u> R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010- 2 <u>3</u> R1.5.2	No change.
CIP-010-1 R2	CIP-010- 2 <u>3</u> 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 <u>3</u> R2.1	No change.
CIP-010-1 R3	CIP-010- 2 <u>3</u> R3	No change.
CIP-010-1 R3.1	CIP-010- 2 <u>3</u> R3.1	No change.
CIP-010-1 R3.2	CIP-010- 2 <u>3</u> 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 <u>3</u> R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010- 2 <u>3</u> R3.2.2	No change.
CIP-010-1 R3.3	CIP-010- 2 <u>3</u> R3.3	No change.
CIP-010-1 R3.4	CIP-010- 2 <u>3</u> R3.4	No change.
NEW	CIP-010- 2 <u>3</u> R4	To respond to the FERC Order No. 791 directive to address transient devices, the SDT modified its approach to use Attachment 1 instead of the table approach. It modified Requirement R4 to “implement one or more documented plan(s) for Transient Cyber Asset and Removable Media that include the applicable elements in Attachment 1, except under CIP Exceptional Circumstances.”
NEW	CIP-010- 2 <u>3</u> , Attachment 1	CIP-010- 2 <u>3</u> Attachment 1 lists the elements required for Transient Cyber Asset and Removable Media Plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the risks posed by transient devices.

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 <u>3</u> 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 <u>3</u> R1.1	No change.
CIP-011-1 R1.2	CIP-011- 2 <u>3</u> R1.2	No change.
CIP-011-1 R2	CIP-011- 2 <u>3</u> R2	No change.
CIP-011-1 R2.1	CIP-011- 2 <u>3</u> R2.1	No change.
CIP-011-1 R2.2	CIP-011- 2 <u>3</u> R2.2	No change.