NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1

November 7, 2011

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	DELETED	Critical Asset Identification – Removed this requirement because new Standard identifies and categorizes BES Cyber Systems directly without declaring assets as critical.
CIP-002-4 R2.	CIP-002-5 R1	Critical Cyber Asset Identification – New Standard identifies BES Cyber Systems as a grouping of Critical Cyber Assets because it allows entities to apply some requirements at a system rather than asset level. BES Cyber Systems are also identified using BES Reliability Operating Services, which provides more detail on what it means for a Cyber Asset to be critical to reliable operation.
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption or cyber assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g. training, response, recovery, etc.). Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.
CIP-002-4 R2.	DELETED	Control Center – No longer applicable since R2 has been deleted.
CIP-002-4 R2.	DELETED	Dial-up Accessible – No longer applicable since R2 has been deleted.
CIP-002-4 R3.	CIP-002-5 R2	Annual Approval – No significant changes.
NEW	CIP-002-5 1.1	Update and re-categorize for changes to BES – Specifies timeframe for complying with all categorization and associated security requirements following a planned change.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 R2	Cyber Security Policy – Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 R2, 2.10	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order 706 paragraph 443.
CIP-003-4 R1.2.	CIP-003-5 R4	The cyber security policy is readily available – The Responsible Entity only needs to make individuals aware of elements of the cyber security policy related to their job function. This was in response to general confusion around the term "readily available". Examples of how to make individuals aware are listed in the Measures.
CIP-003-4 R1.3.	CIP-003-5 R3	Annual review and approval – No significant change.
CIP-003-4 R2.	CIP-003-5 R1	Single senior manager – Created a definition of CIP Senior Manager to prevent cross referencing across Standards.
CIP-003-4 R2.1.	CIP-003-5 R1	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.
CIP-003-4 R2.2.	CIP-003-5 R6	Changes to the CIP Senior Manager and any delegations must be documented within thirty calendar days of the change.

CIP-003-4 R2.3.	CIP-003-5 R5	Delegate authority – Made clear that the CIP Senior Manager can delegate the ability to delegate. For example, a senior manager can delegate the ability to further delegate responsibility for a plant control system to a plant manager.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.
CIP-003-4 R3.1.	DELETED	Requirement R3 is deleted.
CIP-003-4 R3.2.	DELETED	Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Requirement R3 is deleted.
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business. Removed language to “protect” information and replaced with “Implement handling and access control” to clarify the protection that is required.
CIP-003-4 R4.1.	Definition	Identification – Replace this requirement with the defined term BES Cyber System Information.

CIP-003-4 R4.2.	CIP-011-1 1.1	Classification – Removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-1 1.3	Assessment – No significant changes.
CIP-003-4 R5.	CIP-004-5 6.3, CIP-011-1 1.2	Authorize personnel for access to protected information – Clarified the "program for managing access" included the authorization of access as well as handling and access control procedures.
CIP-003-4 R5.1.	DELETED	Authorizing personnel – Personnel are still required to have authorization, and the CIP Senior Manager authorizes or delegates this responsibility. So the additional requirement to have and maintain a list is considered duplicative and unnecessary.
CIP-003-4 R5.1.1.	DELETED	Personnel shall be identified – 5.1 is deleted.
CIP-003-4 R5.1.2.	DELETED	Verification – 5.1 is deleted.
CIP-003-4 R5.2.	CIP-004-5 6.6	Verify access privileges annually – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term annual. Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-011-1 1.3	Annual Review – No significant changes.

CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate Standard because of the additional requirements necessary for satisfying FERC directives and the subject matter is currently spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material and moved example mechanisms to guidance..
CIP-004-4 R2.	CIP-004-5 R2, R3	Training - Addition of identifying the roles that require training. Adding specific role-based training for the visitor control program and storage media as part of the handling of BES Cyber Systems information. Also added the FERC Order 706-directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.1.	CIP-004-5 3.1	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 2.1-2.10	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 2.2	Proper use of CCAs – Minor wording changes. Changed to address cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 2.3,2.4	Physical and electronic access controls training – No significant changes.
CIP-004-4 R2.2.3.	CIP-004-5 2.6	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media
CIP-004-4 R2.2.4.	CIP-004-5 2.7,2.8,2.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order 706 paragraph 413.

CIP-004-4 R2.3.	CIP-004-5 3.2	Annual training – Replaced Annually with calendar year, not to exceed 15 months. .
CIP-004-4 R3.	CIP-004-5 R4, R5, 5.1	Personnel Risk Assessment –Split into two requirements, R4 to define the PRA program and R5 to implement the program for individuals prior to obtaining authorized access.
CIP-004-4 R3.1.	CIP-004-5 4.1, 4.2	Identification and 7 year criminal check – Addressed interpretation request in guidance. Specified that identify verification is only required for each individual's initial assessment. Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 5.2	Perform the PRA every 7 years.– Removed the "for cause" part of the requirement.
CIP-004-4 R3.3.	CIP-004-5 4.4	Addresses the contractor or vendor performed PRA.
CIP-004-4 R4.	CIP-004-5 6.1, 6.2	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 6.4	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

CIP-004-4 R4.2.	CIP-004-5 R7	Prevent further access - The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 2.1	Added to help facilitate understanding what roles the entity has to support the role based training program.
NEW	CIP-004-5 2.5	Visitor control program training – Personnel administering the visitor control program and/or providing escort should have be part of the core training per FERC Order 706 - paragraph 432.
NEW	CIP-004-5 2.10	Electronic interconnectivity training – Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems per FERC Order 706 - paragraph 434.
NEW	CIP-004-5 4.3	PRA failure criteria – There should be documented criteria or a process used to evaluate personnel risk assessments.

NEW	CIP-004-5 7.2	Transfers – The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 7.3	Completion of revocation – The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
NEW	CIP-004-5 7.4	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to guidance.
CIP-005-4a R1.4.	Applicability	Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring cyber assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have an ESP.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.

CIP-005-4a R2.1.	CIP-005-5 1.2	Deny access by default - Changes include referring to the defined term Electronic Access Point and to focus on the entity knowing and having justification for what it allows through the EAP. The requirement explicitly states the network admission control includes both inbound and outbound connections.
CIP-005-4a R2.2.	CIP-007-5 1.1	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 1.3	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of “secure”, which is that the BES Cyber System should not be directly accessible with a phone number only
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant two-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R6	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5
CIP-005-4a R2.5.2.	Measures	The authentication methods - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections. - Evidence requirements are considered as part of the measure.

CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the Standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the Standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process - Evidence requirements are considered as part of the measure.
CIP-005-4a R4.2.	CIP-010-1 3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.

CIP-005-4a R4.3.	CIP-010-1 3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-005-4a R4.4.	CIP-010-1 3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-005-4a R4.5.	CIP-010-1 3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order 706 para 643.
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 4.5	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4

NEW	CIP-005-5 1.6	Inspect & detect potential malicious communications – Per FERC Order 706, paragraph 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
NEW	CIP-005-5 2.1,2.2	Remote Access: intermediate device and encryption– This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for Senior Management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of physically security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 1.2, 1.3	Physical Security Perimeter - Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary.
CIP-006-4c R1.2.	DELETED	No longer requires identifing physical access points and controls at them to reflect the change from Physical Security Perimeter to Defined Physical Boundary
CIP-006-4c R1.3.	CIP-006-5 1.4	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in table row 1.4, which replaces the monitoring term. Otherwise, no significant change.
CIP-006-4c R1.4.	CIP-004-5 2.3	Appropriate use of access controls – The term “appropriate’ is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.
CIP-006-4c R1.5.	CIP-004-5 R6 and R7	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.

CIP-006-4c R1.6.1.	CIP-006-5 2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the applicability section of each security requirement and added this as a defined term in the glossary.
CIP-006-4c R2.1.	Applicability	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the applicability section of each security requirement. For this particular requirement see CIP-006-5 item 1.1
CIP-006-4c R2.2.	Applicability	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the applicability section of each security requirement.
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the applicability section of each security requirement.

CIP-006-4c R4.	CIP-006-5 1.2, 1.3	Physical Access Controls - Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary. Also addressed FERC Order 706 defense in depth. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R5.	CIP-006-5 1.4, 1.5, 1.6	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R6.	CIP-006-5 1.7	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the Defined Physical Boundary. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R7.	CIP-008-5 Evidence Retention	Retain relevant incident related log information is addressed in CIP-008-5
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing
CIP-006-4c R8.1.	CIP-006-5 3.1	Physical access control system 3 yr. testing and maintenance – Shortened periodicity of testing to 2 years to address FERC Order 706 paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of item 3.1.
CIP-006-4c R8.3.	CIP-006-5 3.2	Retain outage records – No significant changes.
NEW	CIP-006-5 1.1	Entity based Operational or procedural controls to restrict physical access – To allow for programmatic protection controls as a baseline for Low Impact BES Cyber Assets and Physical Access Control Systems. This does not require detailed lists of individuals with access.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 1.4	Assess security controls following changes - Provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order ,paragraphs 397, 609, 610, and 611
CIP-007-4 R1.1.	CIP-010-1 1.4	Test procedures – See description and justification for CIP-007-4 R1.
CIP-007-4 R1.2.	CIP-010-1 1.4	Testing reflects production environment - See description and justification for CIP-007-4 R1.
CIP-007-4 R1.3.	CIP-010-1 1.4	The Responsible Entity shall document test results. - See description and justification for CIP-007-4 R1.
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.
CIP-007-4 R2.1.	CIP-007-5 1.1	Enable only those ports and services required for normal and emergency operations – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.2.	CIP-007-5 1.1, 1.2	Disable other ports/services – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.

CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording or CIP-007-4 R3, R3.1, and R3.2 was separated into individual line items to provide more granularity. The documentation of a source (s) to monitor for release of security related patches, hotfixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.
CIP-007-4 R3.1.	CIP-007-5 2.2	Assess patches – Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "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" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.
CIP-007-4 R3.2.	CIP-007-5 2.3	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3, 3.4, 3.5	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of cyber assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in paragraph 619-622 of FERC Order 706, and in particular 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…" In paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.
CIP-007-4 R4.1.	CIP-007-5 R3, 3.1, 3.2, 3.3	Malware prevention tools – See description and justification for CIP-007-4 R4.
CIP-007-4 R4.2.	CIP-007-5 3.4	Update malicious code detections – See description and justification for CIP-007-4 R4.

CIP-007-4 R5.	CIP-007-5 5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase “that minimize the risk of unauthorized access” was removed and more appropriately captured in the rationale statement.
CIP-007-4 R5.1.	CIP-004-5 6.1	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a “need to know” basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5	Access authorization – CIP-003-5 R5 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.
CIP-007-4 R5.1.2.	CIP-007-5 4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.

CIP-007-4 R5.1.3.	CIP-004-5 6.5	Annual account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-007-4 R5.2.	CIP-007-5 5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.
CIP-007-4 R5.2.1.	CIP-007-5 5.4	Change default vendor passwords – The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 5.2	Identify account types and determine acceptable use
CIP-007-4 R5.2.3.	CIP-007-5 5.3	Identify account types and determine acceptable use – No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

CIP-007-4 R5.3.	CIP-007-5 5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters . The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 5.5	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.
CIP-007-4 R6.1.	CIP-007-5 4.1	Identify security events – This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.

CIP-007-4 R6.2.	CIP-007-5 4.2	Identify security events for real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 4.4	Retain relevant log information – No significant changes.
CIP-007-4 R6.5.	CIP-007-5 4.3	Review logs – Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 2.1	Erase media no longer needed to store protected information – Consistent with FERC Order 706, paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word “erase” as, depending on the media itself, erasure may not be sufficient to meet this goal. Removed requirement explicitly requiring records of destruction/redeployment because this was implied as a measure of compliance.
CIP-007-4 R7.1.	CIP-011-1 2.2	Disposal – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.2.	CIP-011-1 2.1	Redeployment – See description and justification for CIP-007-4 R7.

CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 3.1, 3.2	Ports and services review – As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-007-4 R8.3.	CIP-010-1 3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-007-4 R8.4.	CIP-010-1 3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order 706, paragraph 643.
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 1.2	Restrict physical I/O ports – In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

NEW	CIP-007-5 2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.
NEW	CIP-007-5 4.3	Generate real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 5.6	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

NEW	CIP-007-5 R6	Limit malicious code on maintenance devices – This is a new requirement to address the FERC Order 706 paragraph 621 directive to protect against personnel introducing malicious code into the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protective (Protected??) Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code or creating an additional electronic access point.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4 where individual aspects of maintaining the plan are listed as separate requirements. The requirement to have an Incident Response Plan now applies to all Responsible Entities as a foundational element of a cyber security program for BES Cyber Systems.
CIP-008-4 R1.1.	CIP-008-5 1.1	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5.
CIP-008-4 R1.2.	CIP-008-5 1.2	Roles and responsibilities of incident response teams – No significant changes.
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – Coordinating with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single Standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.
CIP-008-4 R1.4.	CIP-008-5 3.3	Update incident response plan following review – Included additional specification on update of response plan Addresses FERC Order 706 Paragraph 686 directive to modify on lessons learned and aspects of the DHS Controls.
CIP-008-4 R1.5.	CIP-008-5 3.1	Review incident response plans annually – No significant changes.
CIP-008-4 R1.6.	CIP-008-5 2.1	Test incident response plans annually – No significant changes.
CIP-008-4 R2.	DELETED	Cyber Security Incident Documentation – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.

NEW	CIP-008-5 3.5	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 3.1	Recovery Plan – Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.
CIP-009-4 R1.1.	CIP-009-5 1.1	Conditions for activation of recovery plan – Reworded to address FERC Order 706 paragraph 694 directive and simplified the requirement.
CIP-009-4 R1.2.	CIP-009-5 1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 2.1	Test recovery plan annually – No significant changes.
CIP-009-4 R3.	CIP-009-5 3.2	Review results of recovery plan activities (tests, events) – Added the timeframe for update.
CIP-009-4 R4.	CIP-009-5 1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 2.2	Test information used for recovery – Combined Requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order 706 directives 739 and 748 related to testing of backups.
NEW	CIP-009-5 1.4	Testing of backup media – Addresses FERC Order 706 paragraph 739 and 748 directives regarding the testing of backup media.
NEW	CIP-009-5 1.6	Process to preserve data for analysis – Added requirement to address FERC Order 706, paragraph 706 regarding the necessity to have procedures in place to retain cyber asset evidence as part of the recovery planning.

NEW	CIP-009-5 3.5	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.

Standard: New Requirements in CIP-010-1 and CIP-011-1		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.
NEW	CIP-010-1 2.1	Monitor for changes to the baseline configuration – Monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This change addresses FERC Order 706, paragraph 397 directive and is based on a review of DHS Catalog of Security Controls (or NIST 800-53).
NEW	CIP-010-1 3.2	Live Vulnerability Assessment – Addresses FERC Order 706 paragraph 541, 542, 544 and 547 directives regarding the performance of a live vulnerability assessment in a test environment.
NEW	CIP-010-1 3.3	Perform active VA on new BES Cyber Assets - Addresses FERC Order 706 paragraph 541, 542, 544 and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.