CIP Standards Draft 4 as of November 5, 2012
CIP Applicability Overview

Key: External Routable Connectivty [2] | Electronic Access Point | With Dial-up | Locally Mounted Hardware

							Applicability										
Std	R	Full Text	Identify, Assess and Correct [1]	Low / High Only	TFE / Dev. Cap.	Sr. Manager / Exc. Circum.	Each Responsible Entity	Each Responsible Entity, for its assets identified in CIP-002-5, Requirement 1.3 (Low) [3]	Medium Impact BES Cyber Systems (MIBCS) [3]	Medium Impact BES Cyber Systems at Control Centers (MIBCS at CC) [3]	High Impact BES Cyber Systems (HIBCS)	EACMS associated with MIBCS	EACMS associated with MIBCS at CC	EACMS associated with HIBCS	PACS associated with MIBCS	PACS associated with MIBCS at CC	PACS associated with HIBCS
002	1	Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3 i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System, and; vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	1.1	Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	1.2	Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	1.3	Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required)	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2.1	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2.2	Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1	-	-	-	Sr	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
002 Total		6	-	-	-	1	6	6	6	6	6	6	6	6	6	6	6
003	1	Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: 1.1 Personnel & training (CIP-004); 1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access; 1.3 Physical security of BES Cyber Systems (CIP-006); 1.4 System security management (CIP-007); 1.5 Incident reporting and response planning (CIP-008); 1.6 Recovery plans for BES Cyber Systems (CIP-009); 1.7 Configuration change management and vulnerability assessments (CIP-010); 1.8 Information protection (CIP-011); and 1.9 Declaring and responding to CIP Exceptional Circumstances.	-	-	-	Sr / Exc. Circum.	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	2.1	Cyber security awareness. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required (Zero Defect and Senior Manager in R Statement)	X	Low	-	Sr	-	Yes	-	-	-	-	-	-	-	-	-
	2.2	Physical security controls. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required (Zero Defect and Senior Manager in R Statement)	X	Low	-	Sr	-	Yes	-	-	-	-	-	-	-	-	-
	2.3	Electronic access controls for external routable protocol connections and Dial-up Connectivity. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required (Zero Defect and Senior Manager in R Statement)	X	Low	-	Sr	-	Yes	-	-	-	-	-	-	-	-	-
	2.4	Incident response to a Cyber Security Incident. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required (Zero Defect and Senior Manager in R Statement)	X	Low	-	Sr	-	Yes	-	-	-	-	-	-	-	-	-
	3	Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	-	-	-	Sr	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4	The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	X	-	-	Sr	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
003 Total		7	5	4	-	7	2	6	3	3	3	2	2	2	2	2	2

CIP Standards Draft 4 as of November 5, 2012
CIP Applicability Overview

Key: External Routable Connectivty [2] | Electronic Access Point | With Dial-up | Locally Mounted Hardware

							Applicability										
Std	R	Full Text	Identify, Assess and Correct [1]	Low / High Only	TFE / Dev. Cap.	Sr. Manager / Exc. Circum.	Each Responsible Entity	Each Responsible Entity, for its assets identified in CIP-002-5, Requirement 1.3 (Low) [3]	Medium Impact BES Cyber Systems (MIBCS) [3]	Medium Impact BES Cyber Systems at Control Centers (MIBCS at CC) [3]	High Impact BES Cyber Systems (HIBCS)	EACMS associated with MIBCS	EACMS associated with MIBCS at CC	EACMS associated with HIBCS	PACS associated with MIBCS	PACS associated with MIBCS at CC	PACS associated with HIBCS
004	1.1	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	2.1	Training content on: 1. Cyber security policies; 2. Physical access controls; 3. Electronic access controls; 4. The visitor control program; 5. Handling of BES Cyber System Information and its storage; 6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 7. Recovery plans for BES Cyber Systems; 8. Response to Cyber Security Incidents; and 9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	2.2	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	X	-	-	Exc. Circum.	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	2.3	Require completion of the training specified in Part 2.1 at least once every 15 calendar months .	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	3.1	A process to confirm identity.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	3.2	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	3.3	Criteria or process to evaluate criminal history records checks for authorizing access.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	3.4	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	3.5	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	4.1	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	X	-	-	Exc. Circum.	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	4.2	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	4.3	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	4.4	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	5.1	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	5.2	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	5.3	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	X	-	-	-	-	-	With ERC	With ERC	Yes	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	5.4	For termination actions, revoke the individual's user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	X	High	-	-	-	-	-	-	Yes	-	-	Yes	-	-	-
	5.5	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	X	High	-	-	-	-	-	-	Yes	-	-	Yes	-	-	-
004 Total		18	17	2	-	2	-	-	16	16	18	15	15	17	15	15	15

CIP Standards Draft 4 as of November 5, 2012
CIP Applicability Overview

Key: External Routable Connectivty [2] | Electronic Access Point | With Dial-up | Locally Mounted Hardware

							Applicability											
Std	R	Full Text	Identify, Assess and Correct [1]	Low / High Only	TFE / Dev. Cap.	Sr. Manager / Exc. Circum.	Each Responsible Entity	Each Responsible Entity, for its assets identified in CIP-002-5, Requirement 1.3 (Low) [3]	Medium Impact BES Cyber Systems (MIBCS) [3]	Medium Impact BES Cyber Systems at Control Centers (MIBCS at CC) [3]	High Impact BES Cyber Systems (HIBCS)	EACMS associated with MIBCS	EACMS associated with MIBCS at CC	EACMS associated with HIBCS	PACS associated with MIBCS	PACS associated with MIBCS at CC	PACS associated with HIBCS
005	1.1	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	-	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	-	-	-	-	-	-
	1.2	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	-	-	-	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	With ERC + assoc. PCA	-	-	-	-	-	-
	1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	-	-	-	-	-	-	EAP	EAP	EAP	-	-	-	-	-	-
	1.4	Where technically feasible perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	-	-	TFE	-	-	-	With DU + assoc. PCA	With DU + assoc. PCA	With DU + assoc. PCA	-	-	-	-	-	-
	1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	-	-	-	-	-	-	-	EAP	EAP	-	-	-	-	-	-
	2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	-	-	TFE	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	-	-	-	-	-	-
	2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	-	-	TFE	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	-	-	-	-	-	-
	2.3	Require multi-factor authentication for all Interactive Remote Access sessions.	-	-	TFE	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	-	-	-	-	-	-
005 Total		8	-	-	4	-	-	-	7	8	8	-	-	-	-	-	-
006	1.1	Define operational or procedural controls to restrict physical access.	X	-	-	-	-	-	Without ERC	Without ERC	-	-	-	-	With ERC	With ERC	Yes
	1.2	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	X	-	-	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	-	With ERC	With ERC	-	-	-	-
	1.3	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	X	High	TFE	-	-	-	-	-	Yes + PCA	-	-	Yes	-	-	-
	1.4	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	X	-	-	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	-	-	-
	1.5	Issue an alarm or alert in response to detected access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	X	-	-	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	-	-	-
	1.6	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	X	-	-	-	-	-	-	-	-	-	-	-	With ERC	With ERC	Yes
	1.7	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	X	-	-	-	-	-	-	-	-	-	-	-	With ERC	With ERC	Yes
	1.8	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	X	-	-	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	-	-	-
	1.9	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	X	-	-	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	-	-	-
	2.1	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	X	-	-	Exc. Circum.	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	-	-	-
	2.2	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	X	-	-	Exc. Circum.	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	-	-	-
	2.3	Retain visitor logs for at least ninety calendar days.	X	-	-	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	-	-	-
	3.1	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	-	-	-	-	-	-	-	-	-	-	-	-	IF ERC + Local Hardware	IF ERC + Local Hardware	Yes + Local Hardware
006 Total		13	12	1	1	2	-	-	9	9	8	8	8	8	4	4	4

CIP Standards Draft 4 as of November 5, 2012
CIP Applicability Overview

Key: External Routable Connectivty [2] | Electronic Access Point | With Dial-up | Locally Mounted Hardware

							Applicability										
Std	R	Full Text	Identify, Assess and Correct [1]	Low / High Only	TFE / Dev. Cap.	Sr. Manager / Exc. Circum.	Each Responsible Entity	Each Responsible Entity, for its assets identified in CIP-002-5, Requirement 1.3 (Low) [3]	Medium Impact BES Cyber Systems (MIBCS) [3]	Medium Impact BES Cyber Systems at Control Centers (MIBCS at CC) [3]	High Impact BES Cyber Systems (HIBCS)	EACMS associated with MIBCS	EACMS associated with MIBCS at CC	EACMS associated with HIBCS	PACS associated with MIBCS	PACS associated with MIBCS at CC	PACS associated with HIBCS
007	1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	X	-	TFE	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	X	-	-	-	-	-	-	Yes	Yes	-	-	-	-	-	-
	2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan, or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	2.4	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	X	-	-	Sr	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	3.1	Deploy method(s) to deter, detect, or prevent malicious code.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	3.2	Mitigate the threat of detected malicious code.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	3.3	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	X	-	Dev. Cap.	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	X	-	Dev. Cap.	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	4.3	Where technically feasible retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	X	-	TFE	Exc. Circum.	-	-	-	Yes + PCA	Yes + PCA	-	Yes	Yes	-	Yes	Yes
	4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	X	High	-	-	-	-	-	-	Yes + PCA	-	-	Yes	-	-	-
	5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	X	-	TFE	-	-	-	With ERC + assoc. PCA	Yes + PCA	Yes + PCA	With ERC	Yes	Yes	With ERC	Yes	Yes
	5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	5.3	Identify individuals who have authorized access to shared accounts.	X	-	-	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	5.4	Change known default passwords, per Cyber Asset capability	X	-	Dev. Cap.	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	X	-	TFE	-	-	-	With ERC + assoc. PCA	With ERC + assoc. PCA	Yes + PCA	With ERC	With ERC	Yes	With ERC	With ERC	Yes
	5.7	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	X	-	TFE	-	-	-	-	Yes + PCA	Yes + PCA	-	Yes	Yes	-	Yes	Yes
007 Total		20	20	1	8	2	-	-	16	19	20	16	18	19	16	18	18

CIP Standards Draft 4 as of November 5, 2012
CIP Applicability Overview

Key: External Routable Connectivty [2] | Electronic Access Point | With Dial-up | Locally Mounted Hardware

							Applicability										
Std	R	Full Text	Identify, Assess and Correct [1]	Low / High Only	TFE / Dev. Cap.	Sr. Manager / Exc. Circum.	Each Responsible Entity	Each Responsible Entity, for its assets identified in CIP-002-5, Requirement 1.3 (Low) [3]	Medium Impact BES Cyber Systems (MIBCS) [3]	Medium Impact BES Cyber Systems at Control Centers (MIBCS at CC) [3]	High Impact BES Cyber Systems (HIBCS)	EACMS associated with MIBCS	EACMS associated with MIBCS at CC	EACMS associated with HIBCS	PACS associated with MIBCS	PACS associated with MIBCS at CC	PACS associated with HIBCS
008	1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	1.2	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	1.4	Incident handling procedures for Cyber Security Incidents.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	2.1	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With a full operational exercise of a Reportable Cyber Security Incident.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	2.2	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	2.3	Retain records related to Reportable Cyber Security Incidents.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	3.1	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1 Document any lessons learned or document the absence of any lessons learned; 3.1.2 Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3 Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
	3.2	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	-	-	-	-	-	-	Yes	Yes	Yes	-	-	-	-	-	-
008 Total		9	-	-	-	-	-	-	9	9	9	-	-	-	-	-	-
009	1.1	Conditions for activation of the recovery plan(s).	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	1.2	Roles and responsibilities of responders.	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	1.3	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	1.4	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	-	-	-	-	-	-	-	Yes	Yes	-	Yes	Yes	-	Yes	Yes
	1.5	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	-	-	Dev. Cap.	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2.1	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	X	-	-	-	-	-	-	Yes	Yes	-	Yes	Yes	-	Yes	Yes
	2.2	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	X	-	-	-	-	-	-	Yes	Yes	-	Yes	Yes	-	Yes	Yes
	2.3	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	X	High	-	-	-	-	-	-	Yes	-	-	-	-	-	-
	3.1	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	-	-	-	-	-	-	-	Yes	Yes	-	Yes	Yes	-	Yes	Yes
	3.2	No later than 60 calendar days after a change to the roles or responsibilities, responders or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	-	-	-	-	-	-	-	Yes	Yes	-	Yes	Yes	-	Yes	Yes
009 Total		10	3	1	1	-	-	-	4	9	10	4	9	9	4	9	9

CIP Standards Draft 4 as of November 5, 2012
CIP Applicability Overview

Key: External Routable Connectivty [2] | Electronic Access Point | With Dial-up | Locally Mounted Hardware

							Applicability										
Std	R	Full Text	Identify, Assess and Correct [1]	Low / High Only	TFE / Dev. Cap.	Sr. Manager / Exc. Circum.	Each Responsible Entity	Each Responsible Entity, for its assets identified in CIP-002-5, Requirement 1.3 (Low) [3]	Medium Impact BES Cyber Systems (MIBCS) [3]	Medium Impact BES Cyber Systems at Control Centers (MIBCS at CC) [3]	High Impact BES Cyber Systems (HIBCS)	EACMS associated with MIBCS	EACMS associated with MIBCS at CC	EACMS associated with HIBCS	PACS associated with MIBCS	PACS associated with MIBCS at CC	PACS associated with HIBCS
010	1.1	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4 Any logical network accessible ports; and 1.1.5. Any security patches applied.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	1.2	Authorize and document changes that deviate from the existing baseline configuration.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	1.3	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	1.4	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3 Document the results of the verification.	X	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	1.5	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	X	High	TFE	-	-	-	-	-	Yes	-	-	-	-	-	-
	2.1	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in CIP-010-1, Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	X	High	-	-	-	-	-	-	Yes + PCA	-	-	Yes	-	-	-
	3.1	At least once every 15 calendar months, conduct a paper or active vulnerability assessment	-	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	3.2	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment , or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	-	High	TFE	-	-	-	-	-	Yes	-	-	-	-	-	-
	3.3	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	-	High	-	Exc. Circum.	-	-	-	-	Yes + PCA	-	-	Yes	-	-	-
	3.4	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	-	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
010 Total		10	6	4	2	1	-	-	6	6	10	6	6	8	6	6	6
011	1.1	Method(s) to identify information that meets the definition of BES Cyber System Information.	X	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	X	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2.1	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	-	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
	2.2	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	-	-	-	-	-	-	Yes + PCA	Yes + PCA	Yes + PCA	Yes	Yes	Yes	Yes	Yes	Yes
011 Total		4	2	-	-	-	-	-	4	4	4	4	4	4	4	4	4
Grand Total		105	65	13	16	15	8	12	80	89	96	61	68	73	57	64	64

Requirements:

Including PCA [3]	-	-	-	-	-	-	38	40	43	-	-	-	-	-	-
With ERC [2]	-	-	-	-	-	-	32	31	1	28	27	-	24	23	-

Notes:

1 In a manner that Identifies, assesses and corrects language located in table statement.

2 Excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity per *"Applicable Systems" Columns in Tables* section of the standards.

3 All of the Cyber Assets and systems, even other BES Cyber Systems of lesser impact, within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP per the *Guidelines and Technical Basis: Requirement R1* section of CIP-005-5.

CIP Standards Draft 4 as of November 5, 2012
CIP Applicability Overview

Reference Tables:

The following tables are for reference purposes to demonstrate how the Applicable Systems from the standards are separated into each individual applicability. Each individual applicability is consolidated into the 11 applicability columns represented in pages 1 through 6 according to the table below. Each consolidated applicability column identifies all standards that apply or could apply to enable a user to reference only one column per asset. For example, the 'Each Responsible Entity' requirements apply to all 11 columns.

Applicable Systems From Standards:

1 Each Responsible Entity
2 Each Responsible Entity, for its high impact and medium impact BES Cyber Systems
3 Electronic Access Points for High Impact BES Cyber Systems
4 Electronic Access Points for Medium Impact BES Cyber Systems
5 Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers
6 High Impact BES Cyber Systems
7 High Impact BES Cyber Systems and their associated: • EACMS
8 High Impact BES Cyber Systems and their associated: • PCA
9 High Impact BES Cyber Systems and their associated: 1. EACMS 2. PACS; and 3. PCA
10 High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS
11 High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA
12 High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA
13 High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA
14 The Responsible Entity
15 Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity
16 Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity
17 Medium Impact BES Cyber Systems
18 Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS 2. PACS; and 3. PCA
19 Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA
20 Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA
21 Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS 2. PACS; and 3. PCA
22 Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS
23 Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA
24 Medium Impact BES Cyber Systems without External Routable Connectivity
25 Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS 2. PACS
26 Medium Impact BES Cyber Systems and their associated: • PCA
27 Medium Impact BES Cyber Systems and their associated: 1. EACMS 2. PACS; and 3. PCA
28 Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS
29 Medium Impact BES Cyber Systems at Control Centers

Individual Applicability Consolidation for Overview:

External Routable Connectivty | Electronic Access Point | With Dial-up | Locally Mounted Hardware

Individual Applicability:	Each Responsible Entity	Each Responsible Entity, for its assets identified in CIP-002-5, Requirement 1.3 (Low)	Medium Impact BES Cyber Systems (MIBCS)	Medium Impact BES Cyber Systems at Control Centers (MIBCS at CC)	High Impact BES Cyber Systems (HIBCS)	EACMS associated with MIBCS	EACMS associated with MIBCS at CC	EACMS associated with HIBCS	PACS associated with MIBCS	PACS associated with MIBCS at CC	PACS associated with HIBCS
High Impact BES Cyber Systems	-	-	-	-	Yes	-	-	-	-	-	-
High Impact BES Cyber Systems with Dial-up Connectivity	-	-	-	-	Yes	-	-	-	-	-	-
High Impact BES Cyber Systems with External Routable Connectivity	-	-	-	-	Yes	-	-	-	-	-	-
PCA associated with HIBCS	-	-	-	-	Yes	-	-	-	-	-	-
PCA associated with HIBCS w DU	-	-	-	-	Yes	-	-	-	-	-	-
PCA associated with HIBCS w ERC	-	-	-	-	Yes	-	-	-	-	-	-
Medium Impact BES Cyber Systems	-	-	Yes	Yes	-	-	-	-	-	-	-
Medium Impact BES Cyber Systems at Control Centers	-	-	-	Yes	-	-	-	-	-	-	-
Medium Impact BES Cyber Systems with Dial-up Connectivity	-	-	Yes	Yes	-	-	-	-	-	-	-
Medium Impact BES Cyber Systems with External Routable Connectivity	-	-	Yes	Yes	-	-	-	-	-	-	-
Medium Impact BES Cyber Systems wo ERC	-	-	Yes	Yes	-	-	-	-	-	-	-
PCA associated with MIBCS w ERC	-	-	Yes	Yes	-	-	-	-	-	-	-
PCA associated with MIBCS	-	-	Yes	Yes	-	-	-	-	-	-	-
PCA associated with MIBCS at CC	-	-	-	Yes	-	-	-	-	-	-	-
PCA associated with MIBCS w DU	-	-	Yes	Yes	-	-	-	-	-	-	-
EACMS associated with MIBCS w ERC	-	-	-	-	-	Yes	Yes	-	-	-	-
EACMS associated with HIBCS	-	-	-	-	-	-	-	Yes	-	-	-
EACMS associated with MIBCS	-	-	-	-	-	Yes	Yes	-	-	-	-
EACMS associated with MIBCS at CC	-	-	-	-	-	-	Yes	-	-	-	-
EAP for HIBCS	-	-	-	-	Yes	-	-	-	-	-	-
EAP for MIBCS	-	-	Yes	Yes	-	-	-	-	-	-	-
EAP for MIBCS at CC	-	-	-	Yes	-	-	-	-	-	-	-
Locally mounted hardware or devices at the PSP associated with HIBCS	-	-	-	-	-	-	-	-	-	-	Yes
Locally mounted hardware or devices at the PSP associated with MIBCS w ERC	-	-	-	-	-	-	-	-	Yes	Yes	-
PACS associated with HIBCS	-	-	-	-	-	-	-	-	-	-	Yes
PACS associated with MIBCS w ERC	-	-	-	-	-	-	-	-	Yes	Yes	-
PACS associated with MIBCS at CC	-	-	-	-	-	-	-	-	-	Yes	-
Each Responsible Entity, for its assets identified in CIP-002-5, Requirement 1.3	-	Yes	-	-	-	-	-	-	-	-	-
Each Responsible Entity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes