Summary of CIP Version 5 Standards

In Version 5 of the Critical Infrastructure Protection ("CIP") Reliability Standards ("CIP Version 5 Standards"), the existing versions of CIP-002 through CIP-009 have been significantly revised, and two new standards, CIP-010 and CIP-011, have been added. These complex standards and accompanying "Guidelines and Technical Basis" now stand at over 300 pages. Please note that while the Federal Energy Regulatory Commission ("FERC") approved these standards in its Order No. 791, it also directed North American Electric Reliability Corporation ("NERC") to develop and file modifications to these standards.

CIP-002-5 – Cyber Security – BES Cyber System Categorization

This revised standard uses a new term to define the assets subject to CIP protections – "BES Cyber System."[1] This standard requires Responsible Entities to implement a process that identifies all BES Cyber Systems impacting the Bulk Electric System as having a high, medium, or low impact. The assets to be considered include Control Centers and backup Control Centers; transmission stations and substations; generation resources; systems and facilities critical to system restoration, including blackstart resources and cranking Paths and initial switching requirements; Special Protection Systems that support the reliable operation of the Bulk Electric System; and for Distribution Providers, specified Protection Systems.

Criteria for Determining Impact Ratings

The detailed criteria for determining impact ratings are set forth in Attachment 1 to the standard. The High Impact category covers Control Centers used to meet the functional obligations of a Reliability Coordinator, a Balancing Authority (for generation equal to or greater than 3000 MW in a single Interconnection or assets that meet criterion 2.3, 2.6, or 2.9 described below), a Transmission Operator for one or more assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10 described below, or a

[1] NERC defines "BES Cyber System" as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC defines "BES Cyber Asset" as follows:

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an [Electronic Security Perimeter ("ESP")], a Cyber Asset within an ESP or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

Generator Operator for one or more assets that meet criterion 2.1, 2.3, 2.6, or 2.9 described below.

The Medium Impact category covers each BES Cyber System not in the High Impact category that meets any of the following criteria (the following list is numbered as it is in Attachment 1 to CIP-002-5):

2.1 Generating units at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single interconnection and that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single interconnection.

2.2 Each BES reactive resource or group of resources at a single location (excluding generation facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater and that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3 Each generation Facility that its Planning Coordinator or Transmission Planner designates as necessary to avoid Adverse Reliability Impact in the planning horizon of more than one year.

2.4 Transmission Facilities operated at 500 kV or higher.[2]

2.5 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6 Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of

[2] For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Interconnection Reliability Operating Limits ("IROLs") and their associated contingencies.

2.7 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8 Transmission Facilities (including generation interconnection Facilities) providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generation Owner as a result of Criterion 2.1 or 2.3 above.

2.9 Each Special Protection System, Remedial Action Scheme, or automated switching System that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable would cause one or more IROLs violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10 Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding or underfrequency load shedding under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11 Each Control Center or backup Control Center not already included in the High Impact Rating that is used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12 Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in the High Impact Rating.

2.13 Each Control Center or backup Control Center not already included in the High Impact Rating that is used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

The Low Impact category covers all other BES Cyber Systems not included in the High Impact or Medium Impact categories that are associated with the following assets and meet the specified applicability qualifications: (1) Control Centers and backup Control Centers; (2) Transmission stations and substations; (3) Generation resources; (4) Systems and facilities critical to system restoration; (5) Special Protection Systems that support the reliable operation of the Bulk Electric System; and (6) for Distribution Providers, specified Protection Systems. The standard indicates that a discrete list of low impact BES Cyber Systems is not required.

Under this standard, the Responsible Entity must review the identifications made under this standard and have its CIP Senior Manager (or delegate) approve those identifications at least once every 15 calendar months. Once the Responsible Entity makes the identifications required by CIP-002-5, it must then comply with the controls included in CIP-003-5 through CIP-011-1 corresponding to each impact category.

CIP-003-5 – Cyber Security – Security Management Controls

This standard requires that each Responsible Entity review and obtain CIP Senior Manager approval at least once every 15 months of documented cyber security policies for its High and Medium Impact BES Cyber Systems that address the following specified topics:

- personnel & training;
- Electronic Security Perimeters, including Interactive Remote Access;
- physical security of BES Cyber Systems;
- system security management;
- incident reporting and response planning;
- recovery plans for BES Cyber Systems;
- configuration change management and vulnerability assessments;
- information protection; and
- declaring and responding to CIP Exceptional Circumstances.[3]

For Low Impact BES Cyber Systems, the standard requires that the Responsible Entity implement "in a manner that identifies, assesses, and corrects deficiencies,"[4] one or more documented cyber security policies that address cyber security awareness, physical security controls, electronic access controls for external routable protocol connections and Dial-up Connectivity, and Cyber Security Incident response. These policies must be reviewed and approved by the CIP Senior Manager at least once every 15 calendar months.

---

[3] A "CIP Exceptional Circumstance" is defined in the NERC Glossary as

> A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

[4] In its Order No. 791, FERC directed NERC to remove this language from 17 requirements and submit its proposal to address FERC's concerns about this language within one year from the effective date of the final rule. FERC believes that this language is ambiguous and results in an unacceptable amount of uncertainty with regard to consistent application, Responsible Entities understanding their obligations, and NERC and the regions providing consistent application in audits and other compliance settings. FERC stated that it understands that the use of this language was a move to a more risk-based model, but FERC believes that a better approach would be to modify NERC's Compliance Monitoring and Enforcement Program.

The standard specifically states that an inventory, list, or discrete identification of Low Impact BES Cyber Systems or their BES Cyber Assets is not required. (The requirement that the Cyber Security Policy be "readily available" was deleted.)

The standard also requires that the CIP Senior Manager be identified by name and that any changes be documented within 30 calendar days of the change. Responsible Entities are also required to implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority unless no delegations are used.

CIP-004-5 – Cyber Security – Personnel and Training

This standard requires documented processes or programs for security awareness, cyber security training, personnel risk assessment, and access management.

Security Awareness

For security awareness, a Responsible Entity must have a program related to High and Medium Impact BES Cyber Systems that at least once each calendar quarter reinforces cyber security practices for personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.

Cyber Security Training

This standard requires that a Responsible Entity implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program that is appropriate to individual roles, functions, or responsibilities that contains the training content listed in the standard.[5] This portion of the standard applies to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity. The training program must require completion of the training prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances, and must require completion of the training at least once every 15 calendar months.

Personnel Risk Assessments

This standard requires that a Responsible Entity implement, in a manner that identifies, assesses, and corrects deficiencies, documented personnel risk assessment

[5] The Standard requires training content on cyber security policies; physical access controls; electronic access controls; visitor control program; handling of BES Cyber System Information and its storage; identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; recovery plans for BES Cyber Systems; response to Cyber Security Incidents; and cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.

programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include each of the following:

- a process to confirm identity;
- a process to perform a seven-year criminal history records check as part of each personnel risk assessment that includes current residence and other locations where, during the seven-year period, the subject has resided for six consecutive months or more;
- criteria or a process to evaluate criminal history records checks for authorizing access;
- criteria or a process for verifying personnel risk assessments performed for contractors or service vendors are conducted according to requirements listed above; and
- a process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

This portion of the standard applies to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity.

Access Management Program

This standard also requires implementation, in a manner that identifies, assesses, and corrects deficiencies, of access management programs for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity that include the following specified requirements:

- a process to authorize electronic access, unescorted physical access into a Physical Security Perimeter, and access to designated storage locations for BES Cyber System Information based on need, except for CIP Exceptional Circumstances;
- verification at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records;
- for electronic access, verification 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; and
- verification at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

Access Revocation Program

In addition, this standard requires a Responsible Entity to implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that include the following specified requirements for High

Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity:

- a process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete removals within 24 hours of the termination action;
- for reassignments or transfers, revocation of the individual's access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires that access;
- for terminations, revocation of the individual's access to the designated storage locations for BES Cyber System Information by the end of the next calendar day following the effective date of the termination;
- for High Impact BES Cyber Systems, a process for terminations, revocation of the individual's non-shared user accounts within 30 calendar days of the effective date of the termination; and
- for High Impact BES Cyber Systems, a process for terminations, change passwords for shared accounts known to the user within 30 calendar days of the termination and for reassignments or transfers, change passwords for shared accounts known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires that access.[6]

CIP-005-5 – Cyber Security – Electronic Security Perimeter(s)

This standard requires Responsible Entities to implement one or more documented processes that include the requirements specified in the standard and listed below:

- for High and Medium Impact BES Cyber Systems, those requirements include that all applicable Cyber Assets connected to a network via a routable protocol must reside with a defined ESP;
- for High and Medium Impact BES Cyber Systems with External Routable Connectivity, the processes must require that all External Routable Connectivity be through an identified Electronic Access Point. (The non-routable blanket exemption has been removed from CIP-002-5.);
- for Electronic Access Points for High and Medium Impact BES Cyber Systems, the processes must require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default;
- for High and Medium Impact BES Cyber Systems with Dial-up Connectivity, where technically feasible, the processes must require that authentication be performed when establishing Dial-up Connectivity with applicable Cyber Assets; and

[6] If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, then the program must require that passwords be changed within 10 calendar days following the end of the operating circumstances.

- for Electronic Access Points for High and Medium Impact BES Cyber Systems, the processes must have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

Interactive Remote Access

The standard also requires that for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity, each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems must implement one or more documented processes that include, where technically feasible, an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset, utilize encryption that terminates at an Intermediate System for all Interactive Remote Access, and require multi-factor authentication for all Interactive Remote Access sessions.

CIP-006-5 – Cyber Security – Physical Security of BES Cyber Systems

This standard requires each Responsible Entity to implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that include the applicable specified requirements.

Physical Security Plan

For Medium Impact BES Cyber Systems without External Routable Connectivity and Physical Access Control Systems associated with High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity, a Responsible Entity is to implement a documented physical security plan that defines operational or procedural controls to restrict physical access.

For Medium Impact BES Cyber Systems with External Routable connectivity, the physical security plan must 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.

For High Impact BES Cyber Systems, where technically feasible, the physical security plan must use two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.

Monitoring for Unauthorized Access

For High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable connectivity, the physical security plan must include monitoring for unauthorized access through a physical access point into a Physical Security Perimeter and issuing an alarm or alert in response to a detected unauthorized 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.

For Physical Access Control Systems associated with High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable connectivity, the physical security plan must include monitoring each Physical Access Control System for unauthorized physical access to a Physical Access Control System and issuing 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 detection. Entry of each individual with authorized unescorted physical access into each Physical Security Perimeter must be logged with information to identify the individual and date and time of entry. Those logs must be retained for at least 90 calendar days.

Visitor Control

This standard also requires each Responsible Entity to implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity that include the applicable specified requirements, including: (1) requiring continuous escorted access of visitors within each Physical Security Perimeter, except during CIP Exceptional Circumstances; (2) requiring manual or automated logging of visitor entry into and exit from the Physical Security Perimeters that includes the 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; and (3) retaining those visitor logs at least 90 calendar days.

Physical Access Control System Maintenance and Testing

The standard also requires each Responsible Entity to implement documented maintenance and testing programs for Physical Access Control Systems for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and locally mounted hardware or devices at the Physical Security Perimeter associated with High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity. Those programs must include 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 are functioning properly.

CIP-007-5 – Cyber Security – Systems Security Management

This standard addresses system security by specifying technical, operational, and procedural requirements in support of protecting High and Medium Impact BES Cyber Systems against compromise that could lead to misoperation or instability of the Bulk Electric System.

Ports & Services

The standard requires each Responsible Entity to implement for High Impact and certain Medium Impact BES Cyber Systems, in a manner that identifies, assesses, and corrects deficiencies, documented processes that collectively address each of the specified requirements related to ports and services. Those requirements include: (1) where technically feasible, enabling only logical network accessible ports that are needed; and (2) protecting against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.

Security Patch Management

This standard requires a Responsible Entity to implement for High and Medium Impact BES Cyber Systems, in a manner that identifies, assesses, and corrects deficiencies, documented processes that collectively address each of the specified requirements related to security patch management. Those requirements include implementing a process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. Security patches must be evaluated at least once every 35 calendar days for applicability. For those patches that are applicable, the Responsible Entity must, within 35 calendar days of the evaluation, apply the applicable patches, create a dated mitigation plan aimed at mitigating the vulnerabilities addressed by each security patch and the timeframe to complete the mitigations, or revise an existing mitigation plan. Each mitigation plan must be implemented within the specified timeframe unless a revision to the plan or an extension of the timeframe is approved by the CIP Senior Manager or delegate.

Malicious Code Prevention

The Responsible Entity must also implement for High and Medium Impact BES Cyber Systems, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that include the specified requirements concerning malicious code prevention (including deploying methods to deter, detect, or prevent malicious code) and mitigation of the threat of detected malicious code. For those methods that use signatures or patterns, the Responsible Entity must have a process for updating the signatures or patterns that also addresses testing and installing the signatures or patterns.

Security Event Monitoring

The Responsible Entity must also implement for High and certain Medium Impact BES Cyber Systems, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that address the specified requirements for security event monitoring, including logging events at the BES Cyber System level or at the Cyber Asset level for identification of, and after-the-fact investigation of, Cyber Security Incidents that include detected successful login attempts, detected failed access attempts and failed login attempts, and detected malicious code.

The processes must include generating alerts for security events that the Responsible Entity determines necessitate an alert, including, at a minimum, detected malicious code and detected failure of event logging. The process must also include retaining, where technical feasible, applicable event logs for at least 90 consecutive calendar days except under CIP Exceptional Circumstances. For High Impact BES Cyber Systems, the Responsible Entity must review a summarization or sampling of logged events at intervals no greater than 15 calendar days to identify Cyber Security Incidents.

System Access Control

The Responsible Entity must implement for High Impact and certain Medium Impact BES Cyber Systems, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that address the specified requirements related to system access control, including:

- having methods to enforce authentication of interactive user access where technically feasible;
- identifying and inventorying all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s);
- identifying individuals who have authorized access to shared accounts;
- changing known default passwords per Cyber Asset capability;
- technically or procedurally enforcing specified password parameters for password-only authentication for interactive user access;
- technically or procedurally enforcing where technically feasible, for password-only authentication for interactive user access, password changes or an obligation to change the password at least once every 15 calendar months; and
- where technically feasible, limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts.

CIP-008-5 – Cyber Security – Incident Reporting and Response Planning

This standard requires each Responsible Entity to document one or more Cyber Security Incident response plans for High and Medium Impact BES Cyber Systems that include the following:

- a process to identify, classify, and respond to Cyber Security Incidents;
- a process to determine if the Cyber Security Incident is a Reportable Cyber Security Incident and notify ES-ISAC within one hour from the determination of a Reportable Cyber Security Incident;
- the roles and responsibilities of Cyber Security Incident response groups or individuals; and
- incident handling procedures for Cyber Security Incidents.

Testing of Cyber Security Incident Response Plan

The standard requires each Responsible Entity to implement its documented Cyber Security Incident response plan for High and Medium Impact BES Cyber Systems to include testing of that plan at least once every 15 calendar months,[7] using that plan when responding to a Reportable Cyber Security Incident, or performing an exercise of a Reportable Cyber Security Incident. The Responsible Entity must also document deviations from the plan taken during the response to the incident or exercise and retain records related to Reportable Cyber Security Incidents.

For High and Medium Impact BES Cyber Systems, within 90 calendar days after completion of the test or an actual Reportable Cyber Security Incident response, Responsible Entities must document any lessons learned or the absence of any lessons learned, update the Cyber Security Incident response plan based on those lessons learned, and notify those with a defined role in the plan of the updates. Within 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that would impact the ability to execute the plan, the plan must be updated and those with a defined role in the plan must be notified.

CIP-009-5 – Cyber Security – Recovery Plans for BES Cyber Systems

This standard specifies the controls needed to protect data that would be useful in the investigation of an event requiring execution of a BES Cyber System recovery plan and requires operational testing to support the recovery of BES Cyber Systems. This standard also establishes a timeline for a Responsible Entity to determine lessons learned and update recovery plans. More specifically, this standard requires each Responsible Entity to have one or more documented recovery plans for High Impact and certain Medium Impact BES Cyber Systems that include the following:

[7] That testing is to be conducted by responding to an actual Reportable Cyber Security Incident, with a paper drill or tabletop exercise of a Reportable Cyber Security Incident, or with an operational exercise of a Reportable Cyber Security Incident.

- conditions for activation of the recovery plan;
- roles and responsibilities of responders;
- one or more processes for the backup and storage of information required to recover BES Cyber System functionality;
- one or more processes to verify the successful completion of the backup processes and to address any backup failures; and
- 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.

This standard further requires each Responsible Entity to implement for High Impact and certain Medium Impact BES Cyber Systems, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan. That plan must include the following: (1) a requirement to test each recovery plan at least once every 15 months;[8] (2) a requirement to test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure it is useable and compatible with current configurations;[9] and (3) for High Impact BES Cyber Systems, a requirement to test each recovery plan at least once every 36 calendar months through an operational exercise of the plan in an environment representative of the production environment.[10]

Each Responsible Entity must also maintain its recovery plans for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers by, not later than 90 calendar days after completion of a recovery plan test or actual recovery, documenting any lessons learned or the absence of any lessons learned, updating the plan, and notifying each person with a defined role in the plan of the updates. Within 60 calendar days after a change to the roles or responsibilities, responders, or technology that would impact the ability to execute the recovery plan, the plan must be updated and those with a defined role in the plan must be notified.

CIP-010-1 – Cyber Security – Configuration Change Management and Vulnerability Assessments

This new standard consolidates the configuration change management and vulnerability assessment from previous versions of CIP-003, CIP-005, and CIP-007. Each Responsible Entity is required to implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes for High and Medium Impact BES Cyber Systems that meet the following specified requirements:

- develop a baseline configuration that includes operating systems or firmware where no independent operation system exists, any commercially available or

[8] This testing is to be conducted by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise.

[9] An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.

[10] An actual recovery response may substitute for an operational exercise.

open-source application software intentionally installed, any custom software installed, any logical network accessible ports, and any security patches applied;

- authorize and document changes that deviate from the existing baseline configuration;
- update the baseline configuration within 30 calendar days of completing a change that deviates from the existing baseline configuration;
- determine, prior to a change that deviates from the existing baseline configuration, the required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change, verify following the change that required cyber security controls are not adversely affected, and document the results of the verification; and
- for High Impact BES Cyber systems, where technically feasible, for each change that deviates from the existing baseline configuration, prior to implementing any change in the production environment, test changes in a test environment or in a production environment where the test is performed in a manner than 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 document the results of the testing.[11]

The standard also requires Responsible Entities to implement for High Impact BES Cyber Systems, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes for configuration monitoring that include monitoring at least once every 35 calendar days for changes to the baseline configuration and documenting and investigating detected unauthorized changes.

This standard requires a Responsible Entity to implement for High and Medium Impact BES Cyber Systems one or more documented processes related to vulnerability assessments that include the specified requirements, including conducting a paper or active vulnerability assessment at least once every 15 calendar months and, where technically feasible, performing an active vulnerability assessment for High Impact BES Cyber Systems at least once every 36 calendar months in a test environment or in a production environment where the test is performed in a manner that minimizes adverse effects and models the baseline configuration of the BES Cyber System in a production environment. The results of the testing must be documented.[12]

[11] If a test environment was used, the differences between the test environment and the production environment must be documented.

[12] If a test environment was used, the differences between the test environment and the production environment must be documented.

For a High Impact BES Cyber System, prior to adding a new applicable Cyber Asset to a production environment, a Responsible Entity must 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. The results of testing and the results of the assessments of both High and Medium Impact BES Cyber Systems must be documented, including the action plan to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completing the action plan, and the execution status of any remediation or mitigation action items.

CIP-011-1 – Cyber Security – Information Protection

This new standard consolidates information protection requirements from previous versions of CIP-003 and CIP-007. It requires each Responsible Entity to implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection programs for High and Medium BES Cyber Systems that must include methods to identify information that meets the definition of BES Cyber System Information and procedures for protecting and securely handling BES Cyber System Information (including storage, transit, and use).

This standard also requires a Responsible Entity to implement one or more documented processes that meet the specified requirements for BES Cyber Asset reuse and disposal. Those processes must require that prior to the release for reuse of the applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. Those processes must also require that prior to the disposal of the applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.