Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAR posted for comment (March 20, 2008 – April 19, 2008)
2. Revised SAR and response to comments approved by SC (July 10, 2008)
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by NERC Board of Trustees (May 6, 2009)
6. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 3 of CIP-002 to CIP-009 final ballot (December 14, 2009)
8. Version 3 of CIP-002 to CIP-009 approved by NERC Board of Trustees (December 16, 2009)
9. Version 4 of CIP-002 posted for informal comment (December 29, 2009)
10. Version 1 of CIP-010 and CIP-011 posted for informal comment (May 3, 2010)

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post for 45-day comment period and pre-ballot review.	7/26/2010
2. Conduct initial ballot.	8/30/2010
3. Post response to comments on initial ballot.	9/10/2010
4. Conduct Second Ballot	10/04/2010
5. Post response to comments on second ballot	10/29/2010
6. Conduct Third (recirculation) ballot.	11/08/2010
7. Submit standard to BOT for adoption.	12/10/2010
8. File standard with regulatory authorities.	12/24/2010

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:

Physical Security Perimeter

Electronic Security Perimeter

A. Introduction

1. Title: Cyber Security — BES Cyber System Protection

2. Number: CIP-011-1

3. Purpose: To ensure Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES.

4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Coordinator

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load-Serving Entity

4.1.10 Distribution Provider

4.1.11 NERC

4.1.12 Regional Entity

5. Effective Date: To be addressed as part of the implementation plan that is currently under development

B. Requirements

Security Governance and Policy (R1)

R1. Each Responsible Entity shall develop, implement, and annually review one or more formal, documented cyber security policies that addresses the following for its BES Cyber Systems:

- **1.1.** Applicability to organizational and third-party personnel;
- **1.2.** Security roles and responsibilities, including those responsible for authorizing access;
- **1.3.** Identification of a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard;
- **1.4.** Personnel training, awareness, and risk assessment;
- **1.5.** Physical security;
- **1.6.** Electronic access control;
- **1.7.** System security;
- **1.8.** Boundary protection;
- **1.9.** Configuration change management;
- **1.10.** Information protection and media sanitization;
- **1.11.** BES Cyber System maintenance;
- **1.12.** Cyber Security Incident response;
- **1.13.** BES Cyber System recovery.

Personnel Training, Awareness, and Risk Assessment (R2 – R4)

R2. Each Responsible Entity shall provide all personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems at least quarterly reinforcement in sound security practices under their security awareness program to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems.

R3. Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access when specified in *CIP-011-1 Table R3 – Cyber Security Training*, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.

For the purpose of this standard, external connectivity is defined as a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System.

For the purpose of this standard, routable protocol is defined as a communications protocol that contains a network address as well as a device address. It allows packets to be forwarded from one network to another.

For the purpose of this standard, non-routable protocol is defined as a communications protocol that contains only a device address and not a network address. It does not incorporate an addressing scheme for sending data from one network to another.

3.1. This cyber security training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems, and include, at a minimum, the following required items:

- The proper use of BES Cyber Systems
- Physical access controls to BES Cyber Systems
- Visitor control program
- The proper handling of BES Cyber Systems information and storage media
- Identification and reporting of a Cyber Security Incident

3.2. For personnel having specified electronic access to any BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems

3.3. For personnel having a role in BES Cyber System recovery this cyber security training shall additionally include those related action plans and procedures to recover or re-establish BES Cyber Systems

3.4. For personnel having a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures

3.5. This Responsible Entity shall maintain documentation that such cyber security training is conducted at least once every 12 months from the date of initial training, including the date the individual's training was completed.

CIP-011-1 Table R3 – Cyber Security Training				
	Cyber Security Training is Required Prior to Obtaining:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
3.1	Electronic access to BES Cyber Systems		Required	Required
3.2	Physical access to BES Cyber Systems with routable external connectivity			Required

R4. Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in *CIP-011-1 Table R4 – Personnel Risk Assessment*, except for program specified exceptional circumstances that impact the reliability of the BES or emergency response, to ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

4.1. This personnel risk assessment program shall at a minimum include:

- Identity verification via photographic identification documentation issued by a government agency (i.e. Federal, State or Provincial)
- A seven year criminal history records check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

4.2. Each Responsible Entity shall document the results of each personnel risk assessment.

4.3. Each Responsible Entity shall update each personnel risk assessment at least once every seven years after the initial personnel risk assessment.

CIP-011-1 Table R4 – Personal Risk Assessment				
	A Personal Risk Assessment is Required Prior to Obtaining:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
4.1	Electronic access to BES Cyber System		Required	Required
4.2	Physical access to BES Cyber Systems with routable external connectivity			Required

Physical Security (R5 – R6)

R5. Each Responsible Entity shall apply the criteria specified in *CIP-011-1 Table R5 – Physical Security for BES Cyber Systems* to prevent and/or detect unauthorized physical access to BES Cyber Systems.

CIP-011-1 Table R5 – Physical Security for BES Cyber Systems				
	Physical Security for BES Cyber Systems shall:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
5.1	Restrict physical access to areas protecting BES Cyber Systems.		Required for external connectivity only	Required
5.2	Monitor physical access to areas protecting BES Cyber Systems.			Required
5.3	Log physical access to areas protecting BES Cyber Systems. Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.			Required
5.4	Log (manual or automated) the entry and exit of visitors (individuals not authorized to have unescorted physical access), including the date and time, to and from the areas protecting BES Cyber Systems.			Required
5.5	Authorize unescorted physical access to areas protecting BES Cyber Systems			Required
5.6	Review authorized unescorted physical access rights to areas protecting BES Cyber Systems on a quarterly basis.			Required
5.7	Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause.			Required
5.8	Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 36 hours.		Control Center only	Control Center only
5.9	Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 72 hours.		generation or Transmission Facility only	generation or Transmission Facility only
5.10	Require continuous escort access of visitors (individuals not authorized to have unescorted physical access) within areas protecting physical access to BES Cyber Systems			Required

CIP-011-1 Table R5 – Physical Security for BES Cyber Systems				
	Physical Security for BES Cyber Systems shall:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
5.11	Review any unauthorized physical access attempts and handle such physical access attempts in accordance with its incident response procedures			Required

R6. Each Responsible Entity shall document and implement one or more physical security plans that apply the criteria specified in *CIP-011-1 Table R6 – Physical Access Control Systems* to prevent and/or detect unauthorized physical access to BES Cyber Systems.

CIP-011-1 Table R6 – Physical Access Control Systems				
	Physical Security Plans shall Require:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
6.1	Restricting physical access to areas protecting physical access control systems identified under Requirement R5, Part 5.1, 5.2, 5.3.		Required for routable connectivity only	Required
6.2	Monitoring physical access to areas protecting physical access control systems identified under Requirement R5, Part 5.1, 5.2, 5.3.		Required for routable connectivity only	Required
6.3	Implementing a maintenance and testing program to ensure that all physical access control systems identified under Requirement R5, Part 5.1, 5.2, 5.3 function properly. The program must include testing and maintenance of all physical security mechanisms on a cycle no longer than three calendar years.		Required for routable connectivity only	Required

Electronic Access Control (R7 – R14)

R7. Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in *CIP-011-1 Table R7– Account Management Specifications* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.

CIP-011-1 Table R7 – Account Management Specifications				
	The Account Management Documentation Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
7.1	Identification of account types, including individual, group, shared, guest, system and administrative accounts, in use for BES Cyber Systems	Required	Required	Required
7.2	Acceptable use of each identified account types	Required	Required	Required

R8. Each Responsible Entity shall apply the criteria specified in *CIP-011-1 Table R8 – Account Management Implementation* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.

CIP-011-1 Table R8 – Account Management Implementation				
	Account Management shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
8.1	Establish and implement a process for authorizing the addition of account(s) and associated access privileges		Required	Required
8.2	Conduct a quarterly review and verification of accounts and associated access privileges			Required
8.3	Monitor the use of shared and guest/anonymous accounts			Required

R9. Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in *CIP-011-1 Table R9 – Access Revocation* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.

CIP-011-1 Table R9 – Access Revocation				
	Revoke System Access Under the Following Conditions:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
9.1	For personnel terminated for cause.	Within 24 hours	Within 24 hours	Within 24 hours
9.2	For personnel who no longer require such access to Control Center BES Cyber Systems		Within 36 hours	Within 36 hours
9.3	For personnel who no longer require such access to Transmission BES Cyber Systems		Within 72 hours	Within 72 hours
9.4	For personnel who no longer require such access to generation BES Cyber Systems		Within 72 hours	Within 72 hours

R10. Each Responsible Entity shall implement the account management access control actions specified in *CIP-011-1 Table R10 – Account Access Control Specifications* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.

CIP-011-1 Table R10 – Account Access Control Specifications				
	Account Access Control Specifications Includes the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
10.1	Change default vendor passwords after installation	Required	Required	Required
10.2	Passwords must be changed at least once every 12 months,	Required	Required	Required
10.3	Implement a password scheme that has the following attributes:[1] Minimum of six characters	Required	Required	Required
10.4	Implement a password scheme that has at least two of the following four attributes:[1] Lower case alphabetic, upper case alphabetic, numeric, “special” characters (e.g. #, $, @, &)		Required	
10.5	Implement a password scheme that has at least three of the following four attributes: [1] Lower case alphabetic, upper case alphabetic, numeric, “special” characters (e.g. #, $, @, &)			Required
10.6	Require that authorized access permissions are the minimum necessary to perform work functions		Required	Required
10.7	Require explicit authorization of access to system and security administrative functions within the BES Cyber System			Required
10.8	Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions			Required

[1] If a device is not capable of meeting the password threshold, then implement the maximum password complexity that the device can support.

R11. Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall implement the requirements included in *CIP-011-1 Table R11 – Wireless and Remote Electronic Access Documentation* to ensure that no unauthorized access is allowed to its BES Cyber Systems.

Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System.

CIP-011-1 Table R11 – Wireless and Remote Electronic Access Documentation				
	Wireless and Remote Electronic Access Documentation Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
11.1	Identify use restrictions for wireless technologies	Required	Required	Required
11.2	If remote access is used and/or implemented, document the allowed methods for remote access	Required for external connectivity only	Required for external connectivity only	Required for external connectivity only
11.3	If remote access is used and/or implemented, establish and implement a defined process for authorizing the establishment of remote access and associated remote access privileges	Required for external connectivity only	Required for external connectivity only	Required for external connectivity only

R12. Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in *CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management* to ensure that no unauthorized access is allowed to its BES Cyber System.

CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management				
	Wireless and Remote Electronic Access Management Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
12.1	If remote access is used and/or implemented, document and implement a quarterly review and verification of the personnel with remote access and their associated access privileges			Required for external connectivity only

R13. Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria specified in *CIP-011-1 Table R13 – Remote Access Revocation* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems

CIP-011-1 Table R13 – Remote Access Revocation				
	Revoke Remote Access Under the Specified Conditions in the Time Frame Identified:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
13.1	Revoke remote access to Control Center BES Cyber Systems when job duties no longer require BES Cyber System remote access.		36 hours for external connectivity only	1 hour for external connectivity only
13.2	Revoke remote access to Transmission substation BES Cyber Systems when job duties no longer require BES Cyber System remote access.		72 hours for external connectivity only	6 hours for external connectivity only
13.3	Revoke remote access to generation BES Cyber Systems when job duties no longer require BES Cyber System remote access.		72 hours for external connectivity only	4 hours for external connectivity only

R14. Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in *CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls* to ensure that no unauthorized access is allowed to its BES Cyber Systems.

CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls				
	Wireless and Remote Electronic Access Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
14.1	If remote access is used and/or implemented, include authentication controls	Required	Required	Required
14.2	If remote access is used and/or implemented, include multifactor authentication controls			Required
14.3	Deny access by default; specify explicit access permissions		Required	Required
14.4	Display an “appropriate use banner” on the user screen of remote electronic access control devices that, upon an interactive attempt to access a BES Cyber System, states that unauthorized use of the system is prohibited.			Required

System Security (R15 – R19)

R15. Each Responsible Entity shall document and implement one or more processes incorporating the criteria specified in *CIP-011-1 Table R15 – Malicious Code* to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions.

CIP-011-1 Table R15 – Malicious Code				
	Malicious Code Protections Shall Consist of Processes to Perform the Following	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
15.1	Limit propagation of malicious code.		Required	Required
15.2	Detect and respond to the introduction of malicious code.		Required	Required
15.3	Implement processes to test and update malicious code protections.		Required	Required

R16. Each Responsible Entity shall document and implement processes incorporating the criteria specified in *CIP-011-1 Table R16 – Security Patch Management* in order to ensure that security vulnerabilities in BES Cyber Systems are mitigated.

CIP-011-1 Table R16 – Security Patch Management				
	Security Patch Management Shall Consist of the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
16.1	Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems.		Required	Required
16.2	Development of an implementation schedule with a fixed date for either installation of the applicable security patches or completion of mitigating measures that address the vulnerability.		Required	Required

R17. Each Responsible Entity shall document and implement processes incorporating the criteria specified in *CIP-011-1 Table R17 – System Hardening* in order to reduce the available attack surface of the BES Cyber System.

CIP-011-1 Table R17 – System Hardening				
	System Hardening Shall Consist of the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
17.1	One or more processes to ensure that only network accessible ports and services used by each BES Cyber System Component required for normal and emergency operations are enabled. In the case where unused network accessible services and communication methods cannot be disabled, the Responsible Entity shall document and implement a mitigation plan.		Required for external connectivity only	Required for external connectivity only
17.2	Disable, or render unusable, externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components.			Required

R18. Each Responsible Entity shall document and implement processes incorporating the criteria specified in *CIP-011-1 Table R18 – Security Event Monitoring* to ensure that security events are known, logged, and responded to on BES Cyber Systems.

CIP-011-1 Table R18 – Security Event Monitoring				
	Security Event Monitoring Shall Consist of the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
18.1	Implement automated tools or organizational processes to monitor and log system events that are related to cyber security for all BES Cyber System components.		Required	Required
18.2	Implement and document one or more security processes for continuous security monitoring that issue alerts for detected system events related to cyber security.		Required	Required
18.3	Maintain logs of system events related to cyber security within the specified time period.		90 calendar days	1 year
18.4	Review logs of system events related to cyber security and maintain records documenting review of logs within the following time periods.		30 calendar days	7 calendar days

R19. Each Responsible Entity shall implement the criteria specified in *CIP-011-1 Table R19 – Communications and Data Integrity* to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems.

CIP-011-1 Table R19 – Communications and Data Integrity				
	Communications and Data Integrity Protection Shall Consist of the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
19.1	Validate data inbound to a BES Cyber System in a Control Center.			Required for external connectivity only
19.2	Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System in a Control Center to determine whether the data has been compromised maliciously.			Required for external connectivity only

Boundary Protection (R20 – R22)

R20. Each Responsible Entity shall document and implement processes that establish electronic access points that incorporate the criteria in *CIP-011-1 Table R20 – Electronic Boundary Protection* to define an electronic security perimeter thereby minimizing the risk of system intrusion.

Electronic access point for the purpose of this standard is defined as a point where electronic access can be controlled for communication paths that transmit and/or receive digital information. All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).

	CIP-011-1 Table R20 – Electronic Boundary Protection			
	Electronic Boundary Protection Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
20.1	Document all communication paths that transmit and/or receive digital information external to each BES Cyber System.	Required	Required	Required
20.2	Establish an electronic access point on each routable protocol or dialup communication path between BES Cyber Systems and other devices that denies access by default and allows explicitly authorized communication.	Required	Required	Required
20.3	Document and implement access control at each electronic access point established in Part 20.2		Required	Required
20.4	Document and implement one or more processes for logging of all authorized remote access and all attempts at or actual unauthorized access at each electronic access point.		Required for external connectivity only	Required for external connectivity only
20.5	Document and implement one or more processes for alerting and review of alerts by designated response personnel on all unauthorized access attempts at each electronic access point within the following time period.		48 hours for external connectivity only	12 hours for external connectivity only
20.6	Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for each BES Cyber System within the following time period.			7 calendar days for external connectivity only

R21. Each Responsible Entity shall document and implement processes that incorporate the criteria in *CIP-011-1 Table R21 – System Boundary Protection* to protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components.

	CIP-011-1 Table R21 – System Boundary Protection			
	System Boundary Protection shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
21.1	Cyber System Components in Control Centers that are shared between BES Cyber Systems must provide logical separation that prevents access between each system.		Required	Required
21.2	Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20.	Required	Required	Required

R22. Each Responsible Entity shall implement the criteria specified in *CIP-011-1 Table R22 – Protective Cyber Systems* to protect each cyber system that establishes physical or electronic boundaries of BES Cyber Systems.

	CIP-011-1 Table R22 – Protective Cyber Systems			
	Protective Cyber Systems shall:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
22.1	Have remote access restricted as specified in Requirement R14 – Wireless and Remote Electronic Access Controls.	Required	Required	Required
22.2	Implement processes and procedures as specified in Requirement R16 -Security Patch Management			Required
22.3	Implement processes and procedures as specified in Requirement R18 -Security Event Monitoring			Required
22.4	Be changed only by authorized personnel in accordance with Requirement R23 - Configuration Change Management		Required	Required

Configuration Change Management (R23)

R23. Each Responsible Entity shall document and implement processes that incorporate the criteria in *CIP-011-1 Table R23 – Configuration Change Management* to prevent and detect unauthorized modifications to BES Cyber Systems.

CIP-011-1 Table R23 – Configuration Change Management				
	Configuration Change Management Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
23.1	Develop an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), including its physical location.	Required		
23.2	Develop a baseline configuration of the BES Cyber System, which shall include an inventory of its physical or virtual BES Cyber System Components, physical location, software (including version), active ports and services, any patches, and any custom software/scripts.		Required	Required
23.3	Authorize and document changes to the BES Cyber System that deviate from the existing inventory and update the inventory and other documentation as necessary within 30 days of the change being completed.	Required		
23.4	Authorize and document changes to the BES Cyber System that deviate from the existing baseline configuration and update the baseline configuration and other documentation as necessary within 30 days of the change being completed.		Required	Required
23.5	Assess potentially impacted cyber security controls to verify controls are not adversely affected following a change to the BES Cyber System that deviates from the existing baseline configuration.			Required

CIP-011-1 Table R23 – Configuration Change Management				
	Configuration Change Management Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
23.6	For each change that deviates from the existing baseline configuration: • test the changes to the BES Cyber System in a test environment that closely models the software versions, active ports and services, any patches, and any custom software/scripts included in the baseline configuration of the BES Cyber System to ensure that cyber security controls are not adversely affected; • document the results of the testing and the differences between the test environment and the baseline configuration of the production environment including a description of the measures used to account for any differences in operation between the test and production environments as a result of the baseline divergence.			Required for Control Center only
23.7	Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes.			Required

Information Protection and Media Sanitization (R24 – R25)

R24. Each Responsible Entity shall document and implement one or more processes that incorporate the criteria in *CIP-011-1 Table R24 – Information Protection* to prevent unauthorized access to sensitive information associated with BES Cyber Systems.

For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.

CIP-011-1 Table R24 – Information Protection				
	Information Protection Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
24.1	Identify and classify sensitive information commensurate with its sensitivity and consequence as related to BES Cyber Systems.		Required	Required
24.2	Implement labeling and handling procedures for sensitive information according to its classification level.		Required	Required
24.3	Explicitly authorize personnel for access to sensitive information.		Required	Required
24.4	Revoke access to sensitive information within 24 hours for personnel terminated for cause.		Required	Required
24.5	Verify at least every 12 months that the access privileges to sensitive information reflect authorization.		Required	Required

R25. Each Responsible Entity shall document and implement one or more processes that incorporate the criteria in *CIP-011-1 Table R25 – Media Sanitization* in order to prevent the unauthorized dissemination of BES Cyber System information.

Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which information is recorded and stored.

CIP-011-1 Table R25 – Media Sanitization				
	Media Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
25.1	Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable.		Required	Required

BES Cyber System Maintenance (R26)

R26. Each Responsible Entity shall document and implement processes that incorporate the criteria in *CIP-011-1 Table R26– Maintenance* to prevent unauthorized maintenance on BES Cyber Systems and ensure that systems used for maintenance do not accidently introduce malicious code into the BES Cyber System.

Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System. Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches. Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System.

CIP-011-1 Table R26 – Maintenance				
	Maintenance Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
26.1	Maintain a list of personnel authorized to perform maintenance on the BES Cyber System and allow only authorized personnel to perform maintenance on the BES Cyber System.		Required	Required
26.2	Detect and prevent the introduction and propagation of malicious code on all maintenance devices.		Required	Required

Cyber Security Incident Response (R27 – R29)

R27. Each Responsible Entity shall document and implement one or more BES Cyber Security Incident response plans that incorporate the criteria in *CIP-011-1 Table R27 – Cyber Security Incident Response Plan Specifications* so that responses to Cyber Security Incidents involving BES Cyber Systems can occur.

CIP-011-1 Table R27 – Cyber Security Incident Response Plan Specifications				
	Cyber Security Incident Response Plan Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
27.1	A process for classifying events as Cyber Security Incidents.	Required	Required	Required
27.2	Roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	Required	Required	Required
27.3	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) either directly or through an intermediary.	Required	Required	Required

R28. Each Responsible Entity shall test its BES Cyber Security Incident response plan(s) as specified in *CIP-011-1 Table R28 – Cyber Security Incident Response Plan Testing Specifications* to verify its response plan's effectiveness in responding to a Cyber Security Incident impacting a BES Cyber System.

CIP-011-1 Table R28 – Cyber Security Incident Response Plan Testing Specifications				
	Cyber Security Incident Response Plan Testing Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
28.1	Test the execution of the incident response plan (by responding to an actual incident, or with a paper drill, or with a full operational exercise) at least once every 12 months.		Required	Required

R29. Each Responsible Entity shall review, update and communicate its incident response plan(s) as specified in *CIP-011-1 Table R29 – Cyber Security Incident Response Plan Review, Update, and Communication Specifications* to ensure that the response plan(s) will function as intended and that personnel are aware of any relevant changes.

CIP-011-1 Table R29 – Cyber Security Incident Response Plan Review, Update, and Communication Specifications				
	Cyber Security Incident Response Plan Review, Update, and Communication Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
29.1	Review the incident response plan(s) at least once every 12 months	Required	Required	Required
29.2	Review the results of each incident response plan test or actual incident response within sixty calendar days of the execution, documenting any identified deficiencies or lessons learned associated with the response plan			Required
29.3	Update each incident response plan based on any documented plan deficiencies within thirty calendar days of the review of the execution of the incident response plan			Required
29.4	Update incident response plan(s) within thirty calendar days of any system, organizational, and technology changes that impact the response plan			Required
29.5	Communicate all updates to personnel responsible for the activation and implementation of the incident response plan(s) within thirty calendar days of the update being completed			Required

BES Cyber System Recovery (R30 – R32)

R30. Each Responsible Entity shall create, document, and implement recovery plan(s) for the disruption, compromise or failure of BES Cyber Systems that incorporates the criteria specified in *CIP-011-1 Table R30 – Recovery Plan Specifications* so that BES Cyber Systems can be restored to a defined state.

CIP-011-1 Table R30 – Recovery Plan Specifications				
	Recovery Plan Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
30.1	Conditions for activation of the recovery plan(s)		Required	Required
30.2	Roles and responsibilities of responders, including identification of the personnel responsible for recovery efforts		Required	Required
30.3	Required actions of personnel responsible for recovery efforts			Required
30.4	Processes for the backup, storage and protection of information required to successfully restore a BES Cyber System			Required
30.5	Processes for the restoration of BES Cyber Systems to include the following: • Reinstall and configure any application and system software using its baseline configuration defined in Requirement R23, • Load any information from the most recent, known secure backups, • Conduct a system test to verify functionality			Required

R31. Each Responsible Entity shall test its recovery plan(s) for BES Cyber Systems in accordance with the criteria specified in *CIP-011-1 Table R31 – Recovery Plan Testing Specifications* to verify recovery plan readiness and effectiveness.

CIP-011-1 Table R31 – Recovery Plan Testing Specifications				
	Recovery Plan Testing Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
31.1	Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 24 months.		Required	
31.2	Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 12 months. Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current.			Required
31.3	Conduct an operational exercise at least once every thirty-six months that demonstrates recovery in a representative environment unless an actual incident response occurred within the thirty-six month timeframe that demonstrates readiness			Required

R32. Each Responsible Entity shall review, update and communicate its recovery plan(s) in accordance with the criteria specified in *CIP-011-1 Table R32 – Recovery Plan Review, Update, and Communication Specifications* to ensure that the recovery plan(s) will function as intended and that personnel are aware of any relevant changes.

CIP-011-1 Table R32 – Recovery Plan Review, Update, and Communication Specifications				
	Recovery Plan Review, Update, and Communication Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
32.1	Review the recovery plan(s) at least once every 12 months or when BES Cyber Systems(s) are replaced, documenting any identified deficiencies		Required	Required
32.2	Review the results of each recovery plan test or actual incident recovery within sixty calendar days of the execution, documenting any identified deficiencies or lessons learned		Required	
32.3	Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the execution, documenting any identified deficiencies or lessons learned			Required
32.4	Update the recovery plan(s) based on any documented deficiencies, lessons learned or any system, organizational, and technology changes at least once every 12 months		Required	
32.5	Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review of the execution of the recovery plan			Required
32.6	Update recovery plan(s) within thirty calendar days of any system, organizational, and technology changes			Required
32.7	Communicate all recover plan updates to personnel responsible for the recovery plan efforts within thirty calendar days of the update being completed		Required	Required

C. Measures

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention (to be added)

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1			