

Exhibit A

**CIP Version 2 Reliability Standard Violation Severity Levels Proposed for
Approval;
CIP Version 2 Reliability Standard CIP-003-2 and CIP-006-2
Violation Risk Factor Assignments Proposed for Approval**

Note – this document only shows those VSLs that were changed as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2.

Following the initial ballot, the Severe VSL for CIP-003-2, Requirement R2.3 was modified to change “or” to “and” to correct an error in the VSLs. See yellow highlighted text on page 3.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards (Project 2008-06):

Index:

Standard Number CIP-002-2 Critical Cyber Asset Identification	2
Standard Number CIP-003-2 Security Management Controls	3
Standard Number CIP-004-2 Personnel & Training.....	5
Standard Number CIP-005-2 Electronic Security Perimeter(s).....	7
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....	8
Standard Number CIP-007-2 Systems Security Management.....	16
Standard Number CIP-008-2 Incident Reporting and Response Planning.....	19
Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets	20

Standard Number CIP-002-2 — Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1.	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.3.	N/A	N/A	<p>The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation,</p> <p>OR</p> <p>The document is not approved by the senior manager,</p> <p>OR</p> <p>Changes to the delegated authority are not documented within thirty calendar days of the effective date.</p>	<p>A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager;</p> <p>AND</p> <p>changes to the delegated authority are not documented within thirty calendar days of the effective date.</p>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.4.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3.2.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
R2.	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, implement, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1.	At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
R3.	N/A	The Responsible Entity has a personnel risk assessment	The Responsible Entity has a personnel risk assessment program	The Responsible Entity does not have a documented personnel risk

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.</p>	<p>as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.</p>	<p>assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access.</p> <p>OR</p> <p>The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.</p>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 — Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3, Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.
R2.3.	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created and implemented but did not maintain a physical security plan.</p>	<p>The Responsible Entity did not document, implement, and maintain a physical security plan.</p>
R1.1.	N/A	<p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.</p>	<p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.</p>	<p>The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.</p> <p>OR</p> <p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to the Critical such Cyber Assets within the Electronic Security Perimeter.</p>

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.2.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
R1.6.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7.	N/A	N/A	The Responsible Entity's physical security plan addresses a process for updating the physical security plan within-thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or reconfiguration.
R1.8.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R1.9.	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
R3.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4.	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
R5.	N/A	<p>The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following</p>	<p>The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following</p>	<p>The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:</p>

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-2.
R6.	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. 	<p>method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. 	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. 	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
R7.	The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained physical access logs for less than 45 calendar days.
R8.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2,	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	and R8.3.	R8.3.	R8.3.	

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement) , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1.	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.</p>
R5.1.3.	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.</p>
R7.	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not maintain</p>	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address redeployment as specified in R7.2.</p>	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1.</p>	<p>The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.</p>

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	records as specified in R7.3.			
R9.	N/A	N/A	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.</p>

Standard Number CIP-008-2 — Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

Standard Number CIP-009-2 — Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 30 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2. Only the 15 VRFs shown in red text are “new.” There were no changes to these VRFs based on stakeholder comments.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 2 CIP-002-2 thru CIP-009-2 Standards:

Index:

Standard Number CIP-003-2 Security Management Controls2
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....3

Standard Number CIP-003 — Security Management Controls			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.	LOWER
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2	R2.4.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8.	Annual review of the physical security plan.	LOWER
CIP-006-2	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM
CIP-006-2	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-2	R4.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets 	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been 	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		<p>opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.</p> <ul style="list-style-type: none"> Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	
CIP-006-2	R6.	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4 	LOWER
CIP-006-2	R7.	<p>Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.</p>	LOWER
CIP-006-2	R8.	<p>Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:</p>	MEDIUM
CIP-006-2	R8.1.	<p>Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.</p>	MEDIUM
CIP-006-2	R8.2.	<p>Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.</p>	LOWER
CIP-006-2	R8.3.	<p>Retention of outage records regarding access controls, logging, and monitoring for a</p>	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		minimum of one calendar year.	

Exhibit B

**Record of Development of Proposed CIP Version 2 Reliability Standard
Violation Severity Levels and Violation Risk Factor Assignments**

Project 2008-06 Cyber Security

Activity:

Phase I
Violation Risk Factors (for CIP-003-2 and CIP-006-2) and Violation Severity Levels (CIP-002-2 through CIP-009-2)

Status:
The recirculation ballot for proposed Violation Severity Levels (VSLs) for critical infrastructure protection (CIP) standards CIP-002-2 through CIP-009-2 and Violation Risk Factors (VRFs) for CIP-003-2 and CIP-006-2 ended November 12, 2009.

Quorum: 88.70%
Approval: 94.24%

The ballot pool approved the VSLs and VRFs.

Draft	Action	Dates	Results	Consideration of Comments
Version 2 Violation Severity Levels (for CIP-002-2 through CIP-009-2) Clean (19) Redline to Last Ballot (20) Version 2 Violation Risk Factors (for CIP-003-2 and CIP-006-2) Clean (21) Redline to Last Approval (22)	Recirculation Ballot Info>> (18) Vote>>	11/02/09 - 11/12/09 (closed)	Summary>> (23) Full Record>> (24)	
Version 2 Violation Severity Levels (for CIP-002-2 through CIP-009-2) Clean (9) Redline to Last Ballot (10) Redline to Last Posting (11) Version 2 Violation Risk Factors (for CIP-003-2 and CIP-006-2) Clean (12) Redline to Last Approval (13)	Initial Ballot Info>> (14) Vote>> Pre-ballot Window Info>> (8) Join>>	09/10/09 - 09/21/09 (closed) 08/11/09 - 09/10/09 (closed)	Summary>> (15) Full Record>> (16)	Consideration of Comments (17)

Version 2 Violation
Severity Levels **(2)**
(for CIP-002-2
through CIP-009-2)

Version 2 Violation
Risk Factors **(3)**
(for CIP-003-2 and
CIP-006-2)

**Supporting
Material:**

Complete set of
materials for
commenting on
Project 2008-06 and
Project 2008-14 **(4-
4.5)** (zip)

Comment Period
[Info>>](#) **(1)**

[Submit
Comments>>](#) **(5)**

*Please submit only
one comment form.
The form covers
Project 2008-06 and
Project 2008-14.

03/16/09 - 04/20/09
(closed)

[Comments
Received>>](#) **(6)**

[Consideration of
Comments>>](#) **(7)**



NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

Comment Period Open

March 16–April 20, 2009

Now available at:

http://www.nerc.com/filez/standards/Reliability_Standards_Under_Development.html

[View all cyber security related standards activities >>](#)

Violation Severity Levels (VSLs) and Violation Risk Factors (VRFs) for Standards CIP-002 through CIP-009

The Standard Drafting Teams for Projects 2008-06 (Cyber Security Order 706) and 2008-14 (Cyber Security Violation Severity Levels) have posted the following items relating to NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009 for a comment period **until 8 p.m. on April 20, 2009:**

- Proposed VSLs for Versions 1 and 2 of standards CIP-002 through CIP-009
- Proposed VRFs for Version 2 of standards CIP-003 and CIP-006
- Proposed revision to the scope of the Standard Authorization Request (SAR) for Project 2008-14

Special Notes for this Comment Period

To make things easier, we've combined the questions for both projects into one [comment form](#). Note that you do not have to answer all of the questions. We've also posted a zip file containing Microsoft Word versions of all documents (for both projects) related to the comment period (comment form, proposed VSLs, proposed VRFs, and revisions to the SAR for 2008-14). The single comment form and the zip file are available on both project pages:

Page for Project 2008-06: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Page for Project 2008-14: http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

If you experience any difficulties in using the form, please contact Lauren Koller at 609-452-8060 or Lauren.Koller@nerc.net.

Project Background

The comment form provides a detailed explanation of the stages of the VSLs and VRFs for the standards. Standards CIP-002 through CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels,” and a key aspect of these projects is the replacement of Levels of Non-Compliance with Violation Severity Levels.

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection - Issued January 18, 2008) approved eight Version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the Reliability Standards CIP-002 through CIP-009 to address specific concerns. Included in Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 through CIP-009 before compliance audits begin on July 1, 2009.

Standards Development Process

The [Reliability Standards Development Procedure](#) contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

*For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*



**Proposed Violation Severity Levels for the CIP
 Version 2 Series of Standards (Project 2008-06):**

Note – this document only shows those VSLs that were changed as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2.

Index:

Standard Number CIP-002-2 Critical Cyber Asset Identification	2
Standard Number CIP-003-2 Security Management Controls	3
Standard Number CIP-004-2 Personnel & Training.....	6
Standard Number CIP-005-2 Electronic Security Perimeter(s).....	10
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....	12
Standard Number CIP-007-2 Systems Security Management.....	26
Standard Number CIP-008-2 Incident Reporting and Response Planning.....	31
Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets	32

Standard Number CIP-002-2 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4. (Version 1)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
R4 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology , the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both two or more of the following : the risk-based assessment methodology , the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	N/A	N/A	The Responsible Entity has not assigned a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1. (Version 1)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.3. (Version 1)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exception from the requirements of the cyber security policy as required.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.3 (Proposed changes to align with version 2)	N/A N/A		N/A	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; or changes to the delegated authority are not documented within thirty calendar days of the effective date.
New R2.4 (Proposed to align with version 2)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document as required, exceptions from the requirements of the cyber security policy.
R3.2. (Version 1)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.2 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
R1 (Proposed changes to align with version 2)	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
R2. (Version 1)	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Proposed changes to align with version 2)	The Responsible Entity established (implemented) and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish (implement) nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish (implement), maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1. (Version 1)	At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.
R2.1 (Proposed changes to align with version 2)	At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3. (Version 1)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in sixty (60) days or more of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.
R3 (Proposed changes to align with version 2)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after in sixty (60) days or more of such personnel were being granted such access except in specified circumstances such as an emergency.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5. (Version 1)	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
R1.5 (Proposed changes to align with version 2)	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3, Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.
R2.3. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not maintain a procedure for securing dial-up access to the Electronic

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Security Perimeter(s) where applicable.
R2.3 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity did not implement or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created but did not maintain a physical security plan.</p>	The Responsible Entity did not create and maintain a physical security plan.
R1 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created and implemented but did not maintain a physical security plan.</p>	The Responsible Entity did not create and document, implement, and maintain a physical security plan.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.1. (Version 1)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical Cyber Assets.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical Cyber Assets.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical access to the Critical Cyber Assets.
R1.1 (Proposed changes to align with version 2)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical such Cyber Assets.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical such Cyber Assets.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not deployed and documented alternative measures to control physical to the Critical-such Cyber Assets.
R1.2. (Version 1)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify all access points through each Physical Security Perimeter but not measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.2 (Proposed changes to align with version 2)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.4 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the appropriate use of physical access controls as described in Requirement R3.
R1.4 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the address the appropriate use of physical access controls as described in

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R3.
R1.5 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan does not include either the procedures for reviewing access authorization requests or revocation of access authorization, in accordance with CIP-004 Requirement R4.	The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
R1.5 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan does not include address either the procedures process for reviewing access authorization requests or the process for the process for revocation of access authorization, in accordance with CIP-004- 2 Requirement R4.	The Responsible Entity's physical security plan does not include address the process procedures for reviewing access authorization requests and the process for the process for revocation of access authorization, in accordance with CIP-004- 2 Requirement R4.
R1.6 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for escorted access within the physical security perimeter.
R1.6 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures address the process for continuous continuous escorted access within the physical security perimeter.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration but the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.
R1.7 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan includes addresses a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within 90 thirty calendar days of the completion of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include address a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.8 (Version 1)	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.
R1.8 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Proposed changes to align with version 2)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Version 1)	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.
R2 (Proposed changes to align with version 2)	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
New R2.1 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
New R2.2 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
R3 (Version 1)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirements R3.1 or R3.2.	Requirements R3.1 or R3.2.	OR One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.
R3 (Proposed changes to align with version 2)	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4 (Version 1)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4 (Proposed changes to align with version 2)	N/A	<p>The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5 (Version 1)	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs for at least ninety calendar days.
R5 (Proposed changes to align with version 2)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. <p>OR</p> <p>An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-</p>

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				008-2.
R6 (Version 1)	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include one of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include two of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include any of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.
R6 (Proposed changes to align with version 2)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record 	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by 	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of 	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
New R7 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs in accordance with the requirements of Standard CIP-008-2.
New R8 (Proposed changes to align with version 2)	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.
New R8.1 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
New R8.2 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)
New R8.3 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2 (Proposed changes to align with version 2)	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. (Version 1)	The Responsible Entity established and documented, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established but did not document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish nor document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3 (Proposed changes to	The Responsible Entity established (implemented) and documented, either separately or	The Responsible Entity established (implemented) but did not document , either	The Responsible Entity documented but did not establish (implement) , either	The Responsible Entity did not establish (implement) nor document , either separately or as

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
align with version 2)	as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R4.1. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.</p>
R5.1.3. (Version 1)	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.</p>
R5.1.3 (Proposed changes to align with version 2)	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.</p>

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R7. (Version 1)	The Responsible Entity established formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not maintain records as specified in R7.3.	The Responsible Entity established formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address redeployment as specified in R7.2.	The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R7 (Proposed changes to align with version 2)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not maintain records as specified in R7.3.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.
R9 (Version 1)	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually or the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R9 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>or the The Responsible Entity did not document €changes resulting from modifications to the systems or controls within thirty ninety calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were €changes resulting from modifications to the systems or controls documented within thirty ninety calendar days of the change being completed.</p>

Standard Number CIP-008-2 Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6	The Responsible Entity has not developed a Cyber Security Incident response plan.
R1 (Proposed changes to align with version 2)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3 (Version 1)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.
R3 (Proposed changes to align with version 2)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery

Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	30 but less than or equal to 120 calendar days of the change.	than or equal to 150 calendar days of the change.	than or equal to 180 calendar days of the change.	plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

**Proposed Violation Risk Factor Modifications
Consistent with the Changes Proposed in the
Version 2 CIP-002-2 thru CIP-009-2 Standards:**

Note – this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2. Only the 15 VRFs shown in red text are “new.”

Index:

Standard Number CIP-003-2 Security Management Controls2
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....3

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-003 Security Management Controls			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.	LOWER
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2	R2.3. (New)	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2	R2.4. (New – similar to version 1 R2.3 which was LOWER)	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER

Standard Number CIP-006 Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8. (New – similar to version 1 R1.9 which was LOWER)	Annual review of the physical security plan.	LOWER
CIP-006-2	R2. (New)	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers,	MEDIUM

Standard Number CIP-006 Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		shall:	
CIP-006-2	R2.1. (New)	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2. (New)	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM
CIP-006-2	R3. (New)	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-2	R4. (New – Similar to version 1 R2, R2.1, R2.2, R2.3, and R2.4 combined – which were all MEDIUM)	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets 	MEDIUM
CIP-006-2	R5. (New – Similar to version 1 R3, R3.1, and R3.2 combined – R3)	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring	MEDIUM

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-006 Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
	and R3.1 were MEDIUM and R3.2 was LOWER)	<p>methods shall be used:</p> <ul style="list-style-type: none"> Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	
CIP-006-2	R6. (New – Similar to version 1 R4, R4.1, R4.2, and R4.3 combined – which were all LOWER)	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4 	LOWER
CIP-006-2	R7. New – Similar to version 1 R5 – which was LOWER)	<p>Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.</p>	LOWER
CIP-006-2	R8. (New – Similar to version 1 R6 – which was MEDIUM)	<p>Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:</p>	MEDIUM
CIP-006-2	R8.1.	<p>Testing and maintenance of all physical security mechanisms on a cycle no longer than</p>	MEDIUM

Standard Number CIP-006 Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
	(New – Similar to version 1 R6.1 – which was MEDIUM)	three years.	
CIP-006-2	R8.2. (New – Similar to version 1 R6.2 – which was LOWER)	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-2	R8.3. (New – Similar to version 1 R6.3 – which was LOWER)	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER

**Proposed Violation Severity Levels for the CIP
 Version 2 Series of Standards (Project 2008-06):**

Note – this document only shows those VSLs that were changed as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2.

Index:

Standard Number CIP-002-2 Critical Cyber Asset Identification	2
Standard Number CIP-003-2 Security Management Controls	3
Standard Number CIP-004-2 Personnel & Training.....	6
Standard Number CIP-005-2 Electronic Security Perimeter(s).....	10
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....	12
Standard Number CIP-007-2 Systems Security Management.....	26
Standard Number CIP-008-2 Incident Reporting and Response Planning.....	31
Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets	32

Standard Number CIP-002-2 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4. (Version 1)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
R4 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology , the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both two or more of the following : the risk-based assessment methodology , the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	N/A	N/A	The Responsible Entity has not assigned a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1. (Version 1)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.3. (Version 1)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exception from the requirements of the cyber security policy as required.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.3 (Proposed changes to align with version 2)	N/A N/A		N/A	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; or changes to the delegated authority are not documented within thirty calendar days of the effective date.
New R2.4 (Proposed to align with version 2)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document as required, exceptions from the requirements of the cyber security policy.
R3.2. (Version 1)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.2 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
R1 (Proposed changes to align with version 2)	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
R2. (Version 1)	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Proposed changes to align with version 2)	The Responsible Entity established (implemented) and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish (implement) nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish (implement), maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1. (Version 1)	At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.
R2.1 (Proposed changes to align with version 2)	At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3. (Version 1)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in sixty (60) days or more of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.
R3 (Proposed changes to align with version 2)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after in sixty (60) days or more of such personnel were being granted such access except in specified circumstances such as an emergency.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5. (Version 1)	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
R1.5 (Proposed changes to align with version 2)	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3, Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.
R2.3. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not maintain a procedure for securing dial-up access to the Electronic

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Security Perimeter(s) where applicable.
R2.3 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity did not implement or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created but did not maintain a physical security plan.</p>	The Responsible Entity did not create and maintain a physical security plan.
R1 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created and implemented but did not maintain a physical security plan.</p>	The Responsible Entity did not create and document, implement, and maintain a physical security plan.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.1. (Version 1)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical Cyber Assets.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical Cyber Assets.	<p>The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.</p> <p>OR</p> <p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical access to the Critical Cyber Assets.</p>
R1.1 (Proposed changes to align with version 2)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical such Cyber Assets.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical such Cyber Assets.	<p>The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.</p> <p>OR</p> <p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity</p>

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not deployed and documented alternative measures to control physical to the Critical-such Cyber Assets.
R1.2. (Version 1)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify all access points through each Physical Security Perimeter but not measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.2 (Proposed changes to align with version 2)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.4 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the appropriate use of physical access controls as described in Requirement R3.
R1.4 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the address the appropriate use of physical access controls as described in

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R3.
R1.5 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan does not include either the procedures for reviewing access authorization requests or revocation of access authorization, in accordance with CIP-004 Requirement R4.	The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
R1.5 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan does not include address either the procedures process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004- 2 Requirement R4.	The Responsible Entity's physical security plan does not include address the process procedures for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004- 2 Requirement R4.
R1.6 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for escorted access within the physical security perimeter.
R1.6 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures address the process for continuous escorted access within the physical security perimeter.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration but the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.
R1.7 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan includes addresses a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within 90 thirty calendar days of the completion of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include address a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.8 (Version 1)	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.
R1.8 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Proposed changes to align with version 2)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Version 1)	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.
R2 (Proposed changes to align with version 2)	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
New R2.1 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
New R2.2 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
R3 (Version 1)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirements R3.1 or R3.2.	Requirements R3.1 or R3.2.	OR One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.
R3 (Proposed changes to align with version 2)	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4 (Version 1)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4 (Proposed changes to align with version 2)	N/A	<p>The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5 (Version 1)	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs for at least ninety calendar days.
R5 (Proposed changes to align with version 2)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. <p>OR</p> <p>An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-</p>

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				008-2.
R6 (Version 1)	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include one of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include two of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include any of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.
R6 (Proposed changes to align with version 2)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record 	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by 	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of 	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
New R7 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs in accordance with the requirements of Standard CIP-008-2.
New R8 (Proposed changes to align with version 2)	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.
New R8.1 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
New R8.2 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)
New R8.3 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2 (Proposed changes to align with version 2)	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. (Version 1)	The Responsible Entity established and documented, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established but did not document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish nor document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3 (Proposed changes to	The Responsible Entity established (implemented) and documented, either separately or	The Responsible Entity established (implemented) but did not document , either	The Responsible Entity documented but did not establish (implement) , either	The Responsible Entity did not establish (implement) nor document , either separately or as

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
align with version 2)	as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R4.1. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.</p>
R5.1.3. (Version 1)	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.</p>
R5.1.3 (Proposed changes to align with version 2)	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.</p>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R7. (Version 1)	The Responsible Entity established formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not maintain records as specified in R7.3.	The Responsible Entity established formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address redeployment as specified in R7.2.	The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R7 (Proposed changes to align with version 2)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not maintain records as specified in R7.3.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.
R9 (Version 1)	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually or the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R9 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>or the The Responsible Entity did not document €changes resulting from modifications to the systems or controls within thirty ninety calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were €changes resulting from modifications to the systems or controls documented within thirty ninety calendar days of the change being completed.</p>

Standard Number CIP-008-2 Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6	The Responsible Entity has not developed a Cyber Security Incident response plan.
R1 (Proposed changes to align with version 2)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3 (Version 1)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.
R3 (Proposed changes to align with version 2)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery

Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	30 but less than or equal to 120 calendar days of the change.	than or equal to 150 calendar days of the change.	than or equal to 180 calendar days of the change.	plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:		
Organization:		
Telephone:		
E-mail:		
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	<input type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

*** If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.**

- Agree
 Disagree

Comments:

- 4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

- 5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?**

- Agree
 Disagree

Comments:

- 6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

Standard Authorization Request Form

Title of Proposed Standard Cyber Security Violation Severity Levels (Project 2008-14)	
Request Date	11/03/2008
Approved by Standards Committee 12/16/08	
Revised Date	3/13/09

SAR Requester Information	SAR Type (<i>Check a box for each one that applies.</i>)
Name Larry Bugh	<input type="checkbox"/> New Standard
Primary Contact Larry Bugh	<input checked="" type="checkbox"/> Revision to existing Standard
Telephone (330) 247-3046 Fax (330) 456-3648 Fx	<input type="checkbox"/> Withdrawal of existing Standard
E-mail larry.bugh@rfirst.org	<input type="checkbox"/> Urgent Action

Standards Authorization Request Form

Purpose (Describe what the standard action will achieve in support of bulk power system reliability.)

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection - Issued January 18, 2008) approved eight Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with "Levels of Non-Compliance" instead of "Violation Severity Levels" and now need to be revised before compliance audits begin in 2009. This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the 'Levels of Non-compliance' in the 83 regulatory-approved standards with 'Violation Severity Levels' which also required development of Violation Severity Levels for any new or revised standards.

Proposed project 2008-14 Cyber Security Violation Severity Levels will meet the FERC directives regarding the development of Violation Severity Levels for the cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

NERC, as the ERO, is required to comply with FERC directives. By developing 'Violation Severity Levels' for the CIP-002 thru CIP-009, NERC and the industry, will be compliant with FERC's directive. By adding VSLs to CIP-002 thru CIP-009 the ERO's Sanctions Guidelines will be able to be used as designed. The Sanctions Guidelines use 'Violation Severity Levels' (along with Violation Risk Factors) as starting points in determining a penalty or sanction.

Brief Description (Provide a paragraph that describes the scope of this standard action.)

Develop Violation Severity Levels for reliability standards CIP-002 thru CIP-009 versions 1 and 2 (under development separately), using the standard development process in order to obtain stakeholder consensus on the assignment of Violation Severity Levels for this set of standards.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.)

The drafting team will develop proposed 'Violation Severity Levels' in accordance with the

Standards Authorization Request Form

guidelines for assigning VSL developed by the drafting team for Project 2007-23- Violation Severity Levels for the following set of reliability standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Version 2 of the standards CIP-002 through CIP-009 is being developed separately. To facilitate prompt completion of version 2 of CIP-002 through CIP-009 including VSLs, the drafting team will draft VSLs for both versions 1 and 2 of standards CIP-002 through CIP-009. While drafting the VSLs for this set of reliability standards, the drafting team will also need to take into consideration FERC's Violation Severity Level Order of June 19, 2008 and any related FERC Orders or Rules.

Reliability Functions

The Standard will Apply to the Following Functions <i>(Check box for each one that applies.)</i>		
<input checked="" type="checkbox"/>	Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
<input checked="" type="checkbox"/>	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
<input checked="" type="checkbox"/>	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
<input checked="" type="checkbox"/>	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
<input type="checkbox"/>	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
<input type="checkbox"/>	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
<input type="checkbox"/>	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
<input checked="" type="checkbox"/>	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
<input checked="" type="checkbox"/>	Transmission Owner	Owns and maintains transmission facilities.
<input checked="" type="checkbox"/>	Transmission	Ensures the real-time operating reliability of the transmission

Standards Authorization Request Form

	Operator	assets within a Transmission Operator Area.
<input type="checkbox"/>	Distribution Provider	Delivers electrical energy to the End-use customer.
<input checked="" type="checkbox"/>	Generator Owner	Owns and maintains generation facilities.
<input checked="" type="checkbox"/>	Generator Operator	Operates generation unit(s) to provide real and reactive power.
<input type="checkbox"/>	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
<input type="checkbox"/>	Market Operator	Interface point for reliability functions with commercial functions.
<input checked="" type="checkbox"/>	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles <i>(Check box for all that apply.)</i>	
<input type="checkbox"/>	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
<input type="checkbox"/>	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
<input type="checkbox"/>	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
<input type="checkbox"/>	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
<input type="checkbox"/>	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
<input type="checkbox"/>	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
<input checked="" type="checkbox"/>	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
<input checked="" type="checkbox"/>	8. Bulk power systems shall be protected from malicious physical or cyber attacks.
Does the proposed Standard comply with all of the following Market Interface Principles? <i>(Select 'yes' or 'no' from the drop-down box.)</i>	
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes	
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes	
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes	
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes	

Standards Authorization Request Form

Related Standards

Standard No.	Explanation

Related SARs

SAR ID	Explanation

Regional Variances

Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
SERC	
RFC	
SPP	
WECC	

Standard Authorization Request Form

Title of Proposed Standard Cyber Security Violation Severity Levels (Project 2008-14)	
Request Date	11/03/2008
Approved by Standards Committee 12/16/08	
<u>Revised Date</u>	<u>3/13/09</u>

SAR Requester Information	SAR Type (<i>Check a box for each one that applies.</i>)
Name Larry Bugh	<input type="checkbox"/> New Standard
Primary Contact Larry Bugh	<input checked="" type="checkbox"/> Revision to existing Standard
Telephone (330) 247-3046 Fax (330) 456-3648 Fx	<input type="checkbox"/> Withdrawal of existing Standard
E-mail larry.bugh@rfirst.org	<input type="checkbox"/> Urgent Action

Standards Authorization Request Form

Purpose (Describe what the standard action will achieve in support of bulk power system reliability.)

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection - Issued January 18, 2008) approved eight Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with "Levels of Non-Compliance" instead of "Violation Severity Levels" and now need to be revised before compliance audits begin in 2009. This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the 'Levels of Non-compliance' in the 83 regulatory-approved standards with 'Violation Severity Levels' which also required development of Violation Severity Levels for any new or revised standards.

Proposed project 2008-14 Cyber Security Violation Severity Levels will meet the FERC directives regarding the development of Violation Severity Levels for the cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

NERC, as the ERO, is required to comply with FERC directives. By developing 'Violation Severity Levels' for the CIP-002 thru CIP-009, NERC and the industry, will be compliant with FERC's directive. By adding VSLs to CIP-002 thru CIP-009 the ERO's Sanctions Guidelines will be able to be used as designed. The Sanctions Guidelines use 'Violation Severity Levels' (along with Violation Risk Factors) as starting points in determining a penalty or sanction.

Brief Description (Provide a paragraph that describes the scope of this standard action.)

Develop Violation Severity Levels for reliability standards CIP-002 thru CIP-009 [versions 1 and 2 \(under development separately\)](#), using the standard development process in order to obtain stakeholder consensus on the assignment of Violation Severity Levels for this set of standards.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.)

The drafting team will develop proposed 'Violation Severity Levels' in accordance with the

Standards Authorization Request Form

guidelines for assigning VSL developed by the drafting team for Project 2007-23- Violation Severity Levels for the following set of reliability standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

[Version 2 of the standards CIP-002 through CIP-009 is being developed separately. To facilitate prompt completion of version 2 of CIP-002 through CIP-009 including VSLs, the drafting team will draft VSLs for both versions 1 and 2 of standards CIP-002 through CIP-009.](#) While drafting the VSLs for this set of reliability standards, the drafting team will also need to take into consideration FERC's Violation Severity Level Order of June 19, 2008 and any related FERC Orders or Rules.

Reliability Functions

The Standard will Apply to the Following Functions <i>(Check box for each one that applies.)</i>		
<input checked="" type="checkbox"/>	Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
<input checked="" type="checkbox"/>	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
<input checked="" type="checkbox"/>	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
<input checked="" type="checkbox"/>	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
<input type="checkbox"/> <input checked="" type="checkbox"/>	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
<input type="checkbox"/> <input checked="" type="checkbox"/>	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
<input type="checkbox"/> <input checked="" type="checkbox"/>	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
<input checked="" type="checkbox"/>	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
<input checked="" type="checkbox"/>	Transmission Owner	Owns and maintains transmission facilities.
<input checked="" type="checkbox"/>	Transmission	Ensures the real-time operating reliability of the transmission

Standards Authorization Request Form

	Operator	assets within a Transmission Operator Area.
<input type="checkbox"/>	Distribution Provider	Delivers electrical energy to the End-use customer.
<input checked="" type="checkbox"/>	Generator Owner	Owns and maintains generation facilities.
<input checked="" type="checkbox"/>	Generator Operator	Operates generation unit(s) to provide real and reactive power.
<input type="checkbox"/>	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
<input type="checkbox"/> <input checked="" type="checkbox"/>	Market Operator	Interface point for reliability functions with commercial functions.
<input checked="" type="checkbox"/>	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles <i>(Check box for all that apply.)</i>	
<input type="checkbox"/>	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
<input type="checkbox"/>	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
<input type="checkbox"/>	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
<input type="checkbox"/>	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
<input type="checkbox"/>	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
<input type="checkbox"/>	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
<input checked="" type="checkbox"/>	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
<input checked="" type="checkbox"/>	8. Bulk power systems shall be protected from malicious physical or cyber attacks.
Does the proposed Standard comply with all of the following Market Interface Principles? <i>(Select 'yes' or 'no' from the drop-down box.)</i>	
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes	
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes	
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes	
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes	

Standards Authorization Request Form

Related Standards

Standard No.	Explanation

Related SARs

SAR ID	Explanation

Regional Variances

Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
SERC	
RFC	
SPP	
WECC	

Proposed Violation Severity Levels for the CIP Version 1 Series of Standards (Project 2008-14):

Index:

Standard Number CIP-002-1 Critical Cyber Asset Identification2
Standard Number CIP-003-1 Security Management Controls4
Standard Number CIP-004-1 Personnel & Training.....9
Standard Number CIP-005-1 Electronic Security Perimeter(s).....13
Standard Number CIP-006-1 Physical Security of Critical Cyber Assets21
Standard Number CIP-007-1 Systems Security Management.....26
Standard Number CIP-008-1 Incident Reporting and Response Planning.....35
Standard Number CIP-009-1 Recovery Plans for Critical Cyber Assets36

Standard Number CIP-002-1 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
R1.1	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology does not include procedures but includes evaluation criteria.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but not evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
R1.2	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.
R2.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
R3.	N/A	N/A	The Responsible Entity has developed a list of Critical Cyber Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Cyber Assets even if such list is null.
R3.1	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber

Standard Number CIP-002-1 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Asset List.
R3.2.	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
R3.3.	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
R4.	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Proposed Violation Severity Levels for the CIP Version 1 Series of Standards (Project 2008-14)

Standard Number CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
R1.2.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
R1.3	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
R2.	N/A	N/A	N/A	The Responsible Entity has not assigned a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1.	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date

Standard Number CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				of designation.
R2.2.	N/A	N/A	N/A	Changes to the senior manager were not documented within thirty calendar days of the effective date.
R2.3.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exception from the requirements of the cyber security policy as required.
R3.	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
R3.1.	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).

Standard Number CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.2.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.
R3.3.	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002 through CIP 009) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002 through CIP 009) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement but documented a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R4.1.	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Standard Number CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.2.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
R5.	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement but documented a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
R5.1.	N/A	N/A	N/A	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, business phone but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name, title, business phone nor the information for which they are responsible for authorizing access.

Standard Number CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.2.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
R5.3.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	The Responsible Entity has established but not documented either a change control or configuration management process.	The Responsible Entity has established but not documented a change control and configuration management process.	The Responsible Entity has not established nor documented either a change control or configuration management process.	The Responsible Entity has not established nor documented a change control and configuration management process.

Proposed Violation Severity Levels for the CIP Version 1 Series of Standards (Project 2008-14)

Standard Number CIP-004-1 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
R2.	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1.	At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.
R2.2.	N/A	N/A	The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include two or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.

Standard Number CIP-004-1 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.3.	N/A	N/A	The Responsible Entity did not maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.
R3.	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in sixty (60) days or more of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.
R3.1.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.

Proposed Violation Severity Levels for the CIP Version 1 Series of Standards (Project 2008-14)

Standard Number CIP-004-1 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.2.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
R3.3.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
R4.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 10% or more but less than 15% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 15% or more of the authorized personnel.
R4.1.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with

Standard Number CIP-004-1 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
			personnel.	such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
R4.2.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity did not document one or more access points to the electronic security perimeter(s).	The Responsible Entity did not identify and document all Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter.	The Responsible Entity did not ensure that one or more Critical Cyber Asset resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
R1.2.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.3.	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.6.	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
R2.	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
R2.1.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.2.	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security Perimeter.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did not document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.
R2.3.	N/A	N/A	N/A	The Responsible Entity did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	N/A	N/A	N/A	The Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.6.	<p>The Responsible Entity did not maintain a document identifying the content of the banner.</p> <p>OR</p> <p>Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.</p>	<p>Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.</p>	<p>Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.</p>	<p>Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.</p>
R3.	<p>The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points.</p> <p>OR</p> <p>The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.</p>	<p>The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.</p>	<p>The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.</p>	<p>The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.</p>

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.1.	<p>The Responsible Entity did not document the electronic or manual processes for monitoring and logging access points to dial-up devices.</p> <p>OR</p> <p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring and logging at 5% or more but less than 10% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring and logging at 10% or more but less than 15% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring and logging at 15% or more of the access points to dial-up devices.</p>
R3.2.	N/A	N/A	<p>Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate notification to designated response personnel.</p>	<p>Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses.</p> <p>OR</p> <p>Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days</p>

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	The Responsible Entity performed at least annually a Vulnerability Assessment for more than 95% but less than 100% of access points to the Electronic Security Perimeter(s).	The Responsible Entity performed at least annually a Vulnerability Assessment for more than 90% but less than or equal to 95% of access points to the Electronic Security Perimeter(s).	The Responsible Entity performed at least annually a Vulnerability Assessment for more than 85% but less than or equal to 90% of access points to the Electronic Security Perimeter(s).	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R5.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
R5.1.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
R5.2.	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar days of the change.	controls within ninety calendar days of the change.	controls within ninety calendar days of the change.	calendar days of the change.
R5.3.	N/A	N/A	N/A	The responsible Entity did not retain electronic access logs for at least 90 calendar days.

Standard Number CIP-006-1 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created but did not maintain a physical security plan.</p>	<p>The Responsible Entity did not create and maintain a physical security plan.</p>
R1.1.	N/A	<p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical Cyber Assets.</p>	<p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical Cyber Assets.</p>	<p>The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.</p> <p>OR</p> <p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical access to the Critical Cyber Assets.</p>

Standard Number CIP-006-1 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.2.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify all access points through each Physical Security Perimeter but not measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.3	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
R1.4	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the appropriate use of physical access controls as described in Requirement R3.
R1.5	N/A	N/A	The Responsible Entity's physical security plan does not include either the procedures for reviewing access authorization requests or revocation of access authorization, in accordance with CIP-004 Requirement R4.	The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
R1.6	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for escorted access within the physical security perimeter.

Standard Number CIP-006-1 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7	N/A	N/A	The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration but the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.
R1.8	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.
R1.9	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include a process for ensuring that the physical security plan is reviewed at least annually.

Standard Number CIP-006-1 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.
R3	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2. OR One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.

Standard Number CIP-006-1 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.
R5	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs for at least ninety calendar days.
R6	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include one of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include two of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include any of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	<p>The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, but did not document that testing is performed as required in R1.2.</p> <p>OR</p> <p>The Responsible Entity did not document the test results as required in R1.3.</p>	<p>The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.</p>	<p>The Responsible Entity did not create, implement nor maintain the test procedures as required in R1.1, did not document that testing is performed as required in R1.2, and did not document the test results as required in R1.3.</p>
R2.	N/A	<p>The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.</p>	<p>The Responsible Entity documented but did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.</p>	<p>The Responsible Entity did not establish nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.</p>
R2.1.	<p>The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).</p>
R2.2.	<p>The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the</p>	<p>The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the</p>	<p>The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the</p>	<p>The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic</p>

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Electronic Security Perimeter(s).	Electronic Security Perimeter(s).	Electronic Security Perimeter(s).	Security Perimeter(s).
R2.3.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure or state an acceptance of risk.
R3.	The Responsible Entity established and documented, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established but did not document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish nor document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3.1.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the patches and upgrades.	patches and upgrades.	patches and upgrades.	upgrades.
R3.2.	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of applicable security patches as required in R3.</p> <p>OR</p> <p>Where the applicable patch is not installed, the Responsible Entity did not document the implementation of the patch or compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.</p>
R4.	The Responsible Entity did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1.	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.</p>
R4.2.	The Responsible Entity documented and implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing of the signatures.	The Responsible Entity did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention “signatures.”
R5.	The Responsible Entity did not document but implemented technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented and implemented technical and procedural controls that enforce access authentication and accountability, however those technical and procedural controls are not enforced for all user activity.	The Responsible Entity implemented technical and procedural controls that enforce access authentication but does not provide accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.
R5.1.1.	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
R5.1.3.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.2.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
R5.2.1.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		personnel changes (for example, change in assignment or termination).	personnel changes (for example, change in assignment or termination).	
R5.3.	The Responsible Entity requires and uses passwords but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
R6.	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
R6.2.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6.3.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
R6.4.	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
R6.5.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	The Responsible Entity established formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not maintain records as specified in R7.3.	The Responsible Entity established formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address redeployment as specified in R7.2.	The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R8	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter.

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Security Perimeter.	Security Perimeter.	Security Perimeter.	OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R9	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually or the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.

Standard Number CIP-008-1 Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6	The Responsible Entity has not developed a Cyber Security Incident response plan.
R2	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for two but less than three calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than two calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than one calendar year.	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1.

Standard Number CIP-009-1 Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity has not annually reviewed recovery plan(s) for Critical Cyber Assets.	The Responsible Entity has created recovery plan(s) for Critical Cyber Assets but did not address one of the requirements CIP-009-1 R1.1 or R1.2.	The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-1 R1.1 and R1.2.
R2	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
R3	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	<p>The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.</p> <p>OR</p> <p>The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.</p>

Standard Number CIP-009-1 Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
R5	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

**Proposed Violation Risk Factor Modifications
Consistent with the Changes Proposed in the
Version 2 CIP-002-2 thru CIP-009-2 Standards:**

Note – this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2. Only the 15 VRFs shown in red text are “new.”

Index:

Standard Number CIP-003-2 Security Management Controls2
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....3

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-003 Security Management Controls			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.	LOWER
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2	R2.3. (New)	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2	R2.4. (New – similar to version 1 R2.3 which was LOWER)	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER

Standard Number CIP-006 Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8. (New – similar to version 1 R1.9 which was LOWER)	Annual review of the physical security plan.	LOWER
CIP-006-2	R2. (New)	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers,	MEDIUM

Standard Number CIP-006 Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		shall:	
CIP-006-2	R2.1. (New)	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2. (New)	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM
CIP-006-2	R3. (New)	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-2	R4. (New – Similar to version 1 R2, R2.1, R2.2, R2.3, and R2.4 combined – which were all MEDIUM)	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets 	MEDIUM
CIP-006-2	R5. (New – Similar to version 1 R3, R3.1, and R3.2 combined – R3)	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring	MEDIUM

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-006 Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
	and R3.1 were MEDIUM and R3.2 was LOWER)	<p>methods shall be used:</p> <ul style="list-style-type: none"> Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	
CIP-006-2	R6. (New – Similar to version 1 R4, R4.1, R4.2, and R4.3 combined – which were all LOWER)	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4 	LOWER
CIP-006-2	R7. New – Similar to version 1 R5 – which was LOWER)	<p>Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.</p>	LOWER
CIP-006-2	R8. (New – Similar to version 1 R6 – which was MEDIUM)	<p>Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:</p>	MEDIUM
CIP-006-2	R8.1.	<p>Testing and maintenance of all physical security mechanisms on a cycle no longer than</p>	MEDIUM

Standard Number CIP-006 Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
	(New – Similar to version 1 R6.1 – which was MEDIUM)	three years.	
CIP-006-2	R8.2. (New – Similar to version 1 R6.2 – which was LOWER)	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-2	R8.3. (New – Similar to version 1 R6.3 – which was LOWER)	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:		
Organization:		
Telephone:		
E-mail:		
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	<input type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

*** If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.**

- Agree
 Disagree

Comments:

- 4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

- 5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?**

- Agree
 Disagree

Comments:

- 6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:	Chris Scanlon	
Organization:	Exelon	
Telephone:	630-576-6926	
E-mail:	christopher.Scanlon@exeloncorp.com	
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	X	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input checked="" type="checkbox"/> RFC	<input type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

***If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language
CIP006	R2				<p>Remove the sentence that appears prior to the OR statement as it is not necessary since it is covered by the other VSLs in this requirement.</p> <p>Sentence to eliminate is as follows: A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access.</p>

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

3. **Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.**

Agree

Disagree

Comments:

4. **If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

5. **The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?**

Agree

Disagree

Comments:

6. **If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:		
Organization:		
Telephone:		
E-mail:		
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	X	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	X	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	X	5 — Electric Generators
<input type="checkbox"/> SERC	X	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input checked="" type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Group Comments (Complete this page if comments are from a group.)

Group Name: Bonneville Power Administration
Lead Contact: Denise Koehn
Contact Organization: Transmission Reliability Program
Contact Segment: Transmission
Contact Telephone: 360-418-2533
Contact E-mail: dekoehn@bpa.gov

Additional Member Name	Additional Member Organization	Region*	Segment*
Huy Ngo	Control Cntr HW Design & Maint	WECC	1
Allen Chan	General Counsel	WECC	1,3,5,6
Robin Chung	Generation Support	WECC	3,5,6
Sheree Chambers	Power Scheduling Coordination	WECC	3,5,6
Tina Weber	Power Scheduling Coordination	WECC	3,5,6
Pete Jeter	Security & Emergency Response	WECC	1,3,5,6
Erik Smith	Security & Emergency Response	WECC	1,3,5,6
Dick Winters	Substation Operations	WECC	1
Curt Wilkins	Transmission System Operations	WECC	1
Kelly Hazelton	Transmission System Operations	WECC	1
Jim Domschot	Transmission Work Planning and Evaluation	WECC	1
Jim Jackson	Transmission Work Planning and Evaluation	WECC	1
Kevin Dorning	Tx PSC Technical Services	WECC	1

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

*** If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

CIP-004-1 — Cyber Security — Personnel and Training
CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
CIP-006-1 — Cyber Security — Physical Security
CIP-007-1 — Cyber Security — Systems Security Management
CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.

- (3) the 15 "new" version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert "Row Above" or "Row Below"

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language
CIP-002-2	R 4			The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two or more of the following: 1) The risk-based assessment methodology for the identification of Critical Assets, 2) the list of Critical Assets and 3) the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, or 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-2	R 2.3			Changes to the delegated authority are not documented within thirty calendar days of the effective date.	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager.
CIP-003-2	R 2.4				Exceptions from the requirements of the cyber security policy were

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language
					not authorized by the senior manager or delegate(s) and documented as required.
CIP-004-2	R 2.1	At least one individual but less than 5% of personnel having unescorted access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having unescorted access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having unescorted access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having unescorted access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-005-2	R 2.3			The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-006-2	R 1.1		Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to Cyber Assets within the Electronic Security Perimeter.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language
					Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical access to Cyber Assets within the Electronic Security Perimeter .
CIP-006-2	1.4				The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4 .
CIP-006-2	R 7			The responsible entity did not retain physical access logs for at least ninety calendar days.	The Responsible Entity did not retain electronic access logs related to reportable incidents in accordance with the requirements of Standard CIP-008-2.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.

Agree

Disagree

Comments:

4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?

Agree

Disagree

Comments:

6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

General:

Several of the VSLs for the version 2 standards include "(implemented)" after "established." It is unclear why the parentheses are necessary, and why the VSL does not just state "established and implemented."

CIP-002-2, R4

1. There doesn't seem to be any substantive difference between High and Severe. In fact High indicates that you don't have any of the 3. Severe indicates that they don't have 2 or more, which could actually be less severe than the High. They seem to be reversed. Our first suggestion therefore is that the definitions be switched so that the more egregious violation is listed under Severe and the less egregious is placed in the High.

2. The proposed language change is cumbersome and could lead to a misinterpretation that a risk based methodology is used to identify Critical Cyber Assets. This would be incorrect. The basis for selection of Critical Cyber Assets is their presence within a Critical Asset, whether they are essential to the reliable operation of the Critical Asset and whether they meet the requirements of R3.1, or R3.2, or R3.3. There is no assessment involved that is a pure yes or no process. The risk-based methodology applies to the Critical Assets. We also recommend numbering each of the required elements to make it even clearer. The suggested replacements below are a bit longer, but make it clearer what the VSL statement is saying.

Note: The definitions are also reversed to put them into the proper categories.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Suggested Change High: The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two or more of the following: 1) The risk-based assessment methodology for the identification of Critical Assets, 2) the list of Critical Assets and 3) the list of Critical Cyber Assets (even if such lists are null.)

Suggested Change Severe: The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, or 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)

CIP-003-2, R 2.3

Suggest breaking it out into two VSLs – rather than having it all under “severe” (see table).

CIP-004-2, R 2.1

Suggest adding “unescorted” before “access” to align with wording in the standard (see table).

CIP-005-2, R 2.3

Suggest breaking it out into two VSLs – rather than having it all under “severe”. Also change “or” to “and” (see table).

CIP-006-2, R1.1

Reads poorly, suggested rewording and including “within the Electronic Security Perimeter” to each VSL (see table).

CIP-006-2, R 1.4

Typo – R3 should be R4 to match version 2 standard (see table).

CIP-006-2, R 7

Added a high VSL to correlate to retention of electronic access logs for 90 days, and for severe VSL added “related to reportable incidents” before log (see table).

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:	Greg Rowland	
Organization:	Duke Energy	
Telephone:	704-382-5348	
E-mail:	gdrowland@dukeenergy.com	
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input checked="" type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input checked="" type="checkbox"/>	4 — Transmission-dependent Utilities
<input checked="" type="checkbox"/> RFC	<input type="checkbox"/>	5 — Electric Generators
<input checked="" type="checkbox"/> SERC	<input type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input checked="" type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

***If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
CIP-002-1	R1.1		The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.		
CIP-004-1	R4.2			N/A	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.
CIP-005-1	R2.6		Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.		

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.

Agree

Disagree

Comments:

4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?

Agree

Disagree

Comments:

6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Group Comments (Complete this page if comments are from a group.)			
Group Name:		Northeast Power Coordinating Council	
Lead Contact:		Guy Zito	
Contact Organization:		Northeast Power Coordinating Council	
Contact Segment:		10--Regional Reliability Organizations and Regional Entities	
Contact Telephone:		212-840-1070	
Contact E-mail:		gzito@npcc.org	
Additional Member Name	Additional Member Organization	Region*	Segment*
Ralph Rufrano	New York Power Authority	NPCC	5
Rick White	Northeast Utilities	NPCC	1
Chris de Graffenried	Consolidated Edison Com. Of New York, Inc.	NPCC	1
David Kiguel	Hydro One Networks Inc.	NPCC	1
Randy MacDonald	New Brunswick System Operator	NPCC	2
Roger Champagne	Hydro-Quebec TransEnergie	NPCC	2
Tony Elacqua	New York Independent System Operator	NPCC	2
Manny Couto	National Grid	NPCC	1

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Kathleen Goodman	ISO - New England	NPCC	2
Brian Evans-Mongeon	Utility Services, LLC	NPCC	6
Mike Garton	Dominion Resources Services	NPCC	5
Chris Orzel	FPL/NextEra	NPCC	5
Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
Kurtis Chong	Independent Electricity System Operator	NPCC	2
Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
Mike Gildea	Constellation Energy	NPCC	6
Michael Schiavone	National Grid	NPCC	1
Brian Hogue	Northeast Power Coordinating Council	NPCC	10

***If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
CIP-004	R1	Remove "(implementation)"	Remove "(implementation)"	Remove "(implementation)"	Remove "(implementation)"
CIP-005	R1.1	Remove "(for example dial-up modem)"	Remove "(for example dial-up modem)"	Remove "(for example dial-up modem)"	Remove "(for example dial-up modem)"
CIP-005 and others	R4 and others	VSLs should identify what has not been demonstrated as the Standard calls for. Request that the percentage thresholds be consistent, as in the earlier Requirements that use percentages.	VSLs should identify what has not been demonstrated as the Standard calls for. Request that the percentage thresholds be consistent, as in the earlier Requirements that use percentages.	VSLs should identify what has not been demonstrated as the Standard calls for. Request that the percentage thresholds be consistent, as in the earlier Requirements that use percentages.	VSLs should identify what has not been demonstrated as the Standard calls for. Request that the percentage thresholds be consistent, as in the earlier Requirements that use percentages.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language
CIP-004	R1	should use the same wording as the Standard as in "and implemented"	should use the same wording as the Standard as in "and implemented"	should use the same wording as the Standard as in "and implemented"	should use the same wording as the Standard as in "and implemented"
CIP-006	R1.7	should use the same wording as the Standard	should use the same wording as the Standard	should use the same wording as the Standard	should use the same wording as the Standard

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.**

Agree

Disagree

Comments:

- 4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments: In the CIP-004-1 R1 version 1 VSL the "(implemented)"/"(implement)" should be removed because it is not in the Standard.

Remove "(for example, dial-up modems) from CIP-005-1 R1.1 because examples can be misleading.

Several requirements specify percentage thresholds in their VSLs. What is the basis for those thresholds?

In CIP-005-1 R4, the VSL identifies what has been demonstrated in accordance with the Standard. This is inconsistent with other VSLs that identify what has not been demonstrated. Because of this, the percentage threshold numbers are not consistent.

- 5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?**

Agree

Disagree

Comments:

- 6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments: In CIP-004 the VSLs for R1 should use the same wording as the Standard.

In CIP-006 the VSLs for R1.7 should use the same wording as the Standard.

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:		
Organization:		
Telephone:		
E-mail:		
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	<input type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Group Comments (Complete this page if comments are from a group.)

Group Name: MRO NERC Standards Review Subcommittee
Lead Contact: Michael Brytowski
Contact Organization: MRO
Contact Segment: 10
Contact Telephone: 651-855-1728
Contact E-mail: mj.brytowski@midwestreliability.org

Additional Member Name	Additional Member Organization	Region*	Segment*
Carol Gerou	MP	MRO	1,3,5,6
Neal Balu	WPS	MRO	3,4,5,6
Terry Bilke	MISO	MRO	2
Joe DePoorter	MGE	MRO	3,4,5,6
Ken Goldsmith	ALTW	MRO	4
Jim Haigh	WAPA	MRO	1,6
Terry Harbour	MEC	MRO	1,3,5,6
Joseph Knight	GRE	MRO	1,3,5,6
Scott Nickels	RPU	MRO	3,4,5,6
Dave Rudolph	BEPC	MRO	1,3,5,6
Eric Ruskamp	LES	MRO	1,3,5,6
Pam Sordet	XCEL	MRO	1,3,5,6

*If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.**

Agree

Disagree

Comments:

- 4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

- 5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?**

Agree

Disagree

Comments:

- 6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:	Michael J. Sonnelitter	
Organization:	NextEra™ Energy Resources, LLC	
Telephone:	561-304-5833	
E-mail:	michael.j.sonnelitter@nexteraenergy.com	
NERC Region		Registered Ballot Body Segment
<input checked="" type="checkbox"/> ERCOT	<input type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input checked="" type="checkbox"/> MRO	<input type="checkbox"/>	3 — Load-serving Entities
<input checked="" type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input checked="" type="checkbox"/> RFC	<input checked="" type="checkbox"/>	5 — Electric Generators
<input checked="" type="checkbox"/> SERC	<input type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input checked="" type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input checked="" type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact E-mail:

Additional Member Name	Additional Member Organization	Region*	Segment*

*** If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.

- Agree
- Disagree

Comments:

4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?

- Agree
- Disagree

Comments:

6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments: General comment for both VSL's and VRF's for CIP-006-2, Use of the term "continuous" under R1.6 will need clarification.

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:	Michael Gammon	
Organization:	Kansas City Power & Light	
Telephone:	816-654-1327	
E-mail:	mike.gammon@kcpl.com	
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input checked="" type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input checked="" type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	<input checked="" type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input checked="" type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input checked="" type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact E-mail:

Additional Member Name	Additional Member Organization	Region*	Segment*

***If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Non-compliance' in the 83 regulatory-approved standards with 'Violation Severity Levels' which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs,

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.**

Agree

Disagree

Comments:

- 4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments: If an entity is performing the requested action, lack of documentation should not be sufficient for a VSL greater than moderate. CIP-003 R6 VSL appears to require 2 processes one for configuration management and one for change control, whereas the standard can be interpreted to require only one.

- 5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?**

Agree

Disagree

Comments:

- 6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:	Paul McClay	
Organization:	Tampa Electric Company	
Telephone:	813 225-5287	
E-mail:	pfmcclay@tecoenergy.com	
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input checked="" type="checkbox"/>	1 — Transmission Owners
<input checked="" type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input checked="" type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	<input checked="" type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input checked="" type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

***If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

General Comments

To a large degree, the violation severity levels (VSLs) do not seem to correspond to actual violation circumstances. For example, many of the VSLs are overly severe for violations that may be simple documentation errors:

Under CIP 002, R3: Lack of inclusion of a single critical cyber asset on the list, regardless of whether that asset is effectively protected under the requirements of the standard is a severe VSL under several of the sub-requirements, which is the same as not having a list at all.

This type of severity level assignment is consistent throughout this document. **It appears that the intent is to ensure that documentation is in place for the auditor, rather than to ensure that the overall cyber security program is in place and operating effectively.** In general, severe VSLs should be reserved for more egregious offenses, such as the lack of a program, policy, or procedure altogether or a failure to adequately protect assets, rather than for minor oversights in documentation. We respectfully request that the drafting team re-evaluate the VSLs to allow for a more consistent, measurable basis for severity rather than focusing purely on existence or accuracy of documentation.

A review of the matrix shows 118 severe, 75 high, 57 moderate, and 34 lower VSLs. One would think that there should be a more even distribution among the levels. Since many of the sub-requirements in the standard simply provide more clarification of details within the overall requirement, we suggest that the assessment of severe be reserved for those situations where the top-level requirements are not met at all. Levels lower through higher could then be used based upon the severity of non-compliance to the more detailed sub-requirements. For example, is something mis-documented or ignored altogether? These are two very different situations and should be treated as such.

There is also a lack of consistency from standard to standard in the way the VSLs are documented and applied. For example, some list VSLs for every top level requirement and sub-requirement (which seem like overkill) while others include consideration of the sub-requirements in the VSL for the top level requirement. The VSLs for some of the standards take a measurable approach with consideration given to severity of the violation, while others are very documentation focused. More time should be spent working on a single consistent approach and apply this approach to all standards.

We respectfully request that the drafting team re-evaluate the VSLs to allow for a more consistent, measurable basis for severity rather than focusing purely on existence or accuracy of documentation.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Unfortunately, time constraints have not allowed us to comment on every VSL that give us concern, however we have provided comments on some of the items that we have noted:

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
CIP002	R1				<p>Comment: If the RE did not include all asset types listed in R1.2.1 through R1.2.7 it is a severe VSL. Some entities will not have all of these asset types to consider.</p> <p>Suggested wording: The Responsible Entity did not consider all applicable asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.</p>
CIP002	R3	<p>Comment: Lack of inclusion of a single critical cyber asset on the list, regardless of whether that asset is effectively protected under the requirements of the standards is a severe VSL under several of the sub-requirements, which is the same as not having a list at all. We recommend moving this to Lower level. Consideration should be given as to whether that was due to a documentation error, or if the asset has been protected. Also, realize that if it is documented as a cyber asset rather than a critical cyber asset it still must be protected under the standards. Suggested wording: Less than 5% of Cyber</p>	5% to 10%	10% - 20%	Greater than 20%

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
		<p>Assets essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.</p>			
CIP003	R1	<p>Comment: The VSLs under requirement 1, do not make sense. It is a higher VSL to have missed a single requirement from CIP002 through CIP009 or to not have the policy readily available to all personnel than it is to not have implemented a cyber security policy at all??? We do not believe this should be a VSL, as the actual violation should be related to the individual requirements that are not met. If it is a violation then it surely belongs at a lower severity level than not having a policy at all.</p> <p>Suggested changes: move VSLs as follows:</p>			
CIP003	R1.1	<p>The VSLs under requirement 1, do not make sense. It is a higher VSL to have missed a single requirement from CIP002 through CIP009 or to not have the policy readily available to all personnel than it is to not have implemented a cyber security policy at all.</p>			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
CIP003	R1.2	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.			
CIP003	R1.3	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.		
CIP003	R2	Not identifying the senior manager by name title and address is the same VSL as not having a senior manager at all? Not updating the information within 30 days is also severe. These are documentation issues that should be Lower VSLs. Suggested changes: move VSLs as follows:			
CIP003	R2.1	The senior manager is not identified by name, title, business phone, business address, and date of designation.			
CIP003	R2.2	Changes to the senior manager were not documented within thirty calendar days of the effective date.			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
CIP003	R6	<p>Comment: The wording of these levels is very difficult to follow. It appears as though essentially the same violation is both high and severe.</p> <p>The Responsible Entity has established but not documented a change control process or: The Responsible Entity has established but not documented a configuration management process.</p>	<p>The Responsible Entity has established but not documented both a change control process and configuration management process.</p>	<p>The Responsible Entity has not established and documented a change control process or : The Responsible Entity has not established and documented a configuration management process. (what if they documented but did not implement)</p>	<p>The Responsible Entity has not established and documented a change control process and: The Responsible Entity has not established and documented a configuration management process.</p>
CIP004		<p>Comment: The VSLs for this particular standard appear to take into account the relative severity of the violation much better than the other VSLs in the document. Thought was definitely given to the extent to which the requirement was violated. We recommend that consideration be given to the other sections in this same manner.</p>			
CIP005	R1.1 – R1.3	<p>Comment: The VSLs for these violations should vary depending upon the severity of the actual violation. Mis-documenting the access points should not be severe.</p>			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
		Not documenting and protecting access points should be. Suggested wording changes as follows:			
CIP005	R1.1	Documentation of access points to the Electronic Security Perimeter(s) do not include all externally connected communication end points (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).			Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end points (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s), and such access points have not been protected.
CIP005	R1.2	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity created by did not document an Electronic Security Perimeter for that single access point at the dial-up device.			For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not create an Electronic Security Perimeter for that single access point at the dial-up device.
CIP005	R1.3	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was protected as but not documented as an access point to the Electronic Security Perimeter.			At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not protected as an access point to the Electronic Security Perimeter.
CIP005	R3.1	Comment: This VSL includes logging in the severity level, but the requirement is only for the establishment of monitoring			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
		<p>procedures. Logging is only required under the top level requirement R3. Additionally this should be a lower severity level. By the way, what is a manual logging process for electronic access points, and how could that be an effective control? Suggested wording change:</p>			
CIP005	R3.1	<p>The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices.</p> <p>OR</p> <p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes monitoring at less than 5% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.</p>
CIP005	R4	<p>Comment: This VSL departs from the measurements used for other similar VSLs. For consistency this should use the 5%, 10%, 15% measurements as used in the other VSLs.</p>			
CIP005	R5.3	<p>Comment: There should be varying levels of severity with this requirement. For example if an</p>			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
		<p>entity is missing 1 hour of access logs or one day, or all access logs the VSL is the same.</p> <p>Consideration also needs to be given to the number of access points for which logging must take place and the possibility that a server hardware or software failure could result in lost log data. Did a technical problem (hardware error) occur, human error, an implementation oversight, or ignorance of the requirement? These are all factors that should weigh into the severity level.</p>			
CIP006	R5	<p>Comment: There should be varying levels of severity with this requirement. For example if an entity is missing 1 hour of access logs or one day, or all access logs the VSL is the same.</p> <p>Consideration needs to be given to the number of access points for which logging must take place and the possibility that a server hardware or software failure could result in lost log data. Did a technical problem occur, human error, an implementation oversight, or ignorance of the requirement? These are all factors that should weigh into the severity level.</p>			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
CIP007	R2	<p>Comment: For this requirement it would seem to make more sense to focus on whether or not the program was applied to all critical cyber assets and cyber assets within the ESP Levels high and severe are the same net result, but you get credit for having documented something you are not executing. Suggested wording changes below:</p>			
		<p>The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.</p>	<p>The Responsible Entity established a process to ensure that only those ports and services required for normal and emergency operations are enabled, but failed to exercise this process on less than 5% of critical cyber assets.</p>	<p>The Responsible Entity established a process to ensure that only those ports and services required for normal and emergency operations are enabled, but failed to exercise this process on more than 5% of critical cyber assets</p>	<p>The Responsible Entity did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.</p>

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Time did not permit review of the V2 VSLs. NERC CIP drafting teams should give consideration to the number of items that they have out for review simultaneously at a time when the industry is working to meet the June and December 2009 compliance dates. We would have appreciated more time to review this, the TFE process, V2 of the standards, and all the new guidelines that were recently circulated.

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.**

- Agree
 Disagree

Comments: Time did not permit review, therefore we cannot agree at this time.

- 4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments: See general comments, we really need the VSLs to focus on measuring the effectiveness of the program rather than the existence or accuracy of documentation.

- 5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?**

- Agree
 Disagree

Comments: We believe that these VSLs as currently defined do not truly look at the effectiveness of controls. We believe that the CSDET is in the best position to evaluate the measures for effectiveness of cyber security controls and should perform this function.

- 6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments: We applaud the effort that has gone into this exercise. We know that it is not easy given the time constraints that NERC is facing. However, we feel the impact to the industry of these VSLs warrants that much more consideration be given to this project, and that time must be allowed to ensure that a quality product is delivered. We do not believe this document is at that point yet.

NERC CIP drafting teams should give consideration to the number of items that they have out for review simultaneously at a time when the industry is working to meet the June and December 2009 compliance dates. We would have appreciated more time to review this, the TFE process, V2 of the standards, and all the new guidelines that were recently circulated.

Additionally, we would like to know if the results and aggregated industry comments will be made available to the industry.

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:	Thad Ness	
Organization:	American Electric Power (AEP)	
Telephone:	614-716-2053	
E-mail:	tkness@aep.com	
NERC Region		Registered Ballot Body Segment
<input checked="" type="checkbox"/> ERCOT	<input checked="" type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input checked="" type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input checked="" type="checkbox"/> RFC	<input checked="" type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input checked="" type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input checked="" type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

***If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
CIP-007-1	R4	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-1	R4.1	N/A	N/A	N/A	<p>The Responsible Entity, as technically feasible, did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity, as technically feasible, did</p>

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
					not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.
CIP-007-1	R4.2	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention “signatures.”
CIP-007-1	R5.3.	The Responsible Entity, as technically feasible, requires and uses passwords but only addresses 2 of the requirements in R5.3.1, R5.3.2, R5.3.3.	The Responsible Entity, as technically feasible, requires and uses passwords but only addresses 1 of the requirements in R5.3.1, R5.3.2, R5.3.3.	The Responsible Entity, as technically feasible, requires but does not use passwords as required in R5.3.1, R5.3.2, R5.3.3, and did not demonstrate why it is not technically feasible.	The Responsible Entity, as technically feasible, does not require nor use passwords as required in R5.3.1, R5.3.2, R5.3.3, and did not demonstrate why it is not technically feasible.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.**

- Agree
 Disagree

Comments:

- 4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments: It appears that the severity levels, as drafted, start from the severe level and follow a graduated scale down to the lower VSL. It appears that this is an arbitrary assignment, especially for binary VSLs. We would suggest that, if selected by a default starting position, the VSLs should be centered on the moderate level and expand in either direction as appropriate.

- 5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?**

- Agree
 Disagree

Comments:

- 6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:	Dan Rochester	
Organization:	IESO	
Telephone:	905-855-6363	
E-mail:	dan.rochester@ieso.ca	
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input checked="" type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input type="checkbox"/>	3 — Load-serving Entities
<input checked="" type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	<input type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

*** If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are "new". These "new" VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 "new" version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.

Agree

Disagree

Comments:

4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

We did not fill out any of the tables above since we feel that it would more meaningful to offer the following high-level comments for the SDT's consideration as it revises the VSLs. Table 1, attached, provides a summary assessment of each of the VSLs proposed for the Version 1 CIP standards. Please also refer to Table 1 for the specific examples cited in the comments below.

1. The existing standard structure and quality do not lend themselves to the development of appropriate and effective VSLs. There are still VRFs assigned to the subrequirements which according to FERC need to have VSLs. This makes it very convoluted to develop the main requirement's VSLs which to a good extent depend on the failure to comply with any of the subrequirements which may have multiple levels of VSL themselves. Further, a key problem arises when the main requirement is assign a binary VSL (Severe) while its subrequirements are graded. Often, the main requirement and some of its subrequirements are of similar nature. Hence, a violation of that similar natured requirement will subject an entity to double penalties.

This is the problem we cited in the NERC's filing on the 322 VSL sets in the beginning of the year. The industry will need to continue to deal with this misfit issue until the requirements themselves are revamped and restructured.

The remaining comments provided in the Comment Form are developed ignoring this issue, i.e., the way the standards are written not how they be written, and deal with the VSLs proposed for each main and subrequirement and look for consistency among the VSLs assigned to the requirements.

2. Some VSLs can be graded, but they are treated as binary. Some examples are (not exhaustive): R1 and R1.2 in CIP-002-1, R2 and R4.2 in CIP-003-1, R2.3 and R3.2 in CIP-007-1. Suggestions to grade these requirements and other such requirements are provided in Table 1.
3. Some requirements are assessed complete failure (Severe) if any one of the subrequirements is not met. This is clearly unacceptable since if the argument is that failing one of them essentially fails the bulk of the intent of the main requirement, then what about failing one of the remaining subrequirements? Do they all rise up to the level that failing any one would mean failing the bulk of the intent of the main requirements?

Examples are: R4 in CIP-005-1, R8 in CIP-007. Detailed suggestions to make this change grade are provided in Table 1.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

4. Some subrequirements' violations are "rolled-up" to determine the main requirements' VSLs, which is the proper way. However, this approach is not consistently applied and in some cases where it is applied, there are no VSLs proposed for the subrequirements despite they are assigned VRFs. This is not consistent with the approach applied elsewhere in the CIP standards or the FERC directives. Examples are: R2, R3, R4 and R6 of CIP-006-1, R1 and R7 in CIP-007-1. A consistent approach needs to be applied to all requirements.
5. For requirements of similar nature, some are graded while others are not. This is inconsistent. Some examples re: R2.1 to R2.3 compared to R3.1 to R3.3 in CIP-003-1.
6. Some requirements have listed under it, or included in the sentence, a number of conditions to be met yet the VSLs make no mention of these conditions. Examples are: R1 of CIP-004-1 and R1 of CIP-006-1.

5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?

- Agree
 Disagree

Comments:

6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

Table 2, attached provides a summary assessment of the VRFs and VSLs for the Version 2 CIP standards. Examples cited in the comments below can be found in table 2.

1. Similar problems as identified for the Version 1 CIP standards VSLs are also identified among the VSLs for the Version 2 CIP standards. An added inconsistency is the removal of some of the VSLs for the subrequirements after they are rolled-up to the main requirement. Examples re R2, R6 and R8 in CIP-006-2.
2. Some subrequirements have become bullets. The main requirements' VSLs are dependent on which of the bulleted items are not complied with. It suggests that the bulleted items should in fact be subrequirements (conditions to meet the main requirement). We speculate that the SDT's intent is to roll-up non-compliance of subrequirements to the main requirement's VSLs, the approach is proper but this does not need a change from subrequirements to bullets. The latter is appropriate when the items are not required to be met, but rather they are listed as options or examples.

Table 1
Summary of Comments on VSLs for Version 1 CIP Standards

Standard/ Requirement	Assessment/Comment
CIP-002-1	
R1	R1 is poorly structured. Comment on VSL can only be made based on how it's written, not how it should be written. VSL for R1 is binary, which it shouldn't be. It is a good example of how inappropriate to have a binary requirement while its subrequirements' VSLs are a mixture of binary and graded.
R1.1	Graded, but not based on the failure of its subrequirements.
R1.2 R1.2.1 – R1.2.7	VSL for R1.2 is binary, which could be graded depending on the failure to meet any of its subrequirements.
R2	OK, but the last part “even if such list is null” seems irrelevant.
R3	The VSLs for R3 should be graded to also cover the Low and Moderate columns since it has subrequirements R3.1 to R3.3 all of which need to be met fully comply with R3. Further, the last part “even if such list is null” under the Severe condition seems irrelevant.
R3.1	Binary; OK.
R3.2	Ditto
R3.3	Ditto
R4	OK.
CIP-003-1	
R1	The VSLs are determined w/o regard to any of the subrequirements, which they should.
R1.1	Binary: OK, and hence should form the basis for determining the VSL for R1.
R1.2	Ditto
R1.3	Not binary. In itself OK. These VSLs can also form the basis for determining the VSL for R1.
R2	The VSL should be graded according to how many of R2.1 to R2.3 are missed.
R2.1	OK as a condition to determine R2, but itself can be graded according to which elements are missing.
R2.2	OK as a condition to determine R2, but itself can be graded according to how late the document is issued.
R2.3	OK as a condition to determine R2, but itself can be graded since there are two conditions in this subrequirement.
R3	It doesn't make sense that the Low and Moderate entries are assigned N/A when the VSLs can be further graded to capture the conditions where the responsible entity fails to meet any of R3.1 to R3.3.
R3.1	The VSLs for this and the other two subrequirements seem OK, but it illustrates the inconsistent approach between R2 and R3. The VSLs for R2's subrequirements should be graded in a similar fashion.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R3.2	See above comment.
R3.3	See above comment.
R4	OK, given the nature of the main and subrequirements and the fact that separate VRFs are assigned to them. A more appropriate approach would be to grade R4's VSLs according to the extent to which the responsible entity fails to meet its subrequirements.
R4.1	The VSL starts off at the High level for missing one of the elements. This should be Low. Missing 2 a Moderate, 3 a High, etc.
R4.2	The VSL could be graded according to the percentage of information that is not classified.
R4.3	OK.
R5	OK given the way the main and subrequirements are written and the fact that separate VRFs are assigned to them. A more appropriate approach would be to grade R5's VSLs according to the extent to which the responsible entity fails to meet the subrequirements.
R5.1	The VSL for R5.1 should be graded according to the extent of failure to meet R5.1.1 and R5.1.2 since they are the conditions for fully meeting R5.1.
R5.1.1	Should be graded since there are a number of elements in this subrequirement.
R5.1.2	Should be graded according to the delay in verifying the information.
R5.2	Should be graded according to the delay in completing the review.
R5.3	Should be graded according to the delay in assessing and documenting the processes.
R6	OK.
CIP-004-1	
R1	OK, but could be improved to consider inclusion of the bulleted elements.
R2	OK given the current structure and assignment of VRFs to R2 and its subrequirements.
R2.1	OK
R2.2	Could be improved to stipulate conditions for Low and Moderate since the requirement itself contains several conditions: "...policies, access controls, and procedures". None of them are covered in the High and Severe VSLs.
R2.3	OK.
R3	OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R3.1	OK
R3.2	OK
R3.3	OK
R4	OK given the current structure and assignment of VRFs to R4 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R4.1	OK
R4.2	OK
CIP-005-1	

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R1	OK given the current structure and assignment of VRFs to R1 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R1.1	OK
R1.2	OK
R1.3	OK
R1.4	OK
R1.5	OK
R1.6	OK
R2	OK given the current structure and assignment of VRFs to R2 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R2.1	OK
R2.2	OK
R2.3	OK
R2.4	OK
R2.5	OK
R2.6	OK
R3	OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R3.1	OK
R3.2	OK
R4	OK for the conditions that are independent of R4.1 to R4.4. Assigning a Severe VSL for missing any one (or more) of R4.1 to R4.4 is like treating it a like binary requirement where in fact it can be graded according to how many of R4.1 to R4.4 are missed. Suggest to grade this.
R5	OK given the current structure and assignment of VRFs to R5 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R5.1	OK
R5.2	OK
R5.3	Should be graded according to the number of days that the log was maintained.
CIP-006-1	
R1	The VSLs for R1 should be determined according to the extent of failure to meet any of its subrequirements this requirement, as it is so clearly indicated in R1 that the plan shall address, at a minimum, the subrequirements that follow.
R1.1	O.
R1.2	OK
R1.3	OK as a condition to determine the VSL for R1 but since it is not, the VSLs for R1.3 should be graded according to which element among “processes, tools, and procedures” is missing.
R1.4	OK
R1.5	OK

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R1.6	OK
R1.7	OK
R1.8	OK
R1.9	OK
R2	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R3	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R4	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R5	Should be graded according to the number of days that the log was maintained.
R6	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
CIP-007-1	
R1	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R2	OK given the current structure and assignment of VRFs to R2 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R2.1	OK.
R2.2	OK
R2.3	Should be graded according to the number or % of cases that the responsible entity failed to document compensated measure(s) for those unused ports and services cannot be disabled.
R3	OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R3.1	OK
R3.2	Should be graded according to the number or % of cases that the responsible entity failed to document the implementation of security patches and/or failed to document compensated measure(s) for those patches that are not installed.
R4	OK given the current structure and assignment of VRFs to R4 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R4.1	Should be graded according to the number or % of cases that the responsible entity failed to meet either of the two conditions stipulated in this subrequirements.
R4.2	OK
R5	OK given the current structure and assignment of VRFs to R5 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R5.1	Should be graded according to which of R5.1.1 to R5.1.2 are missed since they are the required elements in the policy.
R5.1.1	OK by itself but it should get rolled up to the determination of VSLs for R5.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R5.1.2	OK by itself but it should get rolled up to the determination of VSLs for R5.
R5.1.3	Binary is OK if it was rolled up to the determination of VSLs for R5. Otherwise, the VSLs should be graded according to the delay in completing the annual review.
R5.2	Disagree with the binary VSL since to fully meet the intent of R5.2, all of its subrequirements must be complied with. The VSLs for R5.2 should be graded according to the extent of failing to meet any of its subrequirements.
R5.2.1	OK
R5.2.2	Should be graded according to the number or % of the individuals that the responsible entity failed to identify.
R5.2.3	OK
R5.3	OK
R6	OK given the current structure and assignment of VRFs to R6 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R6.1	OK
R6.2	OK
R6.3	OK
R6.4	OK
R6.5	Should be graded according to the number or % of the logged cases that the responsible entity failed to review and provided records documenting the review.
R7	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R8	OK for the conditions that are independent of R8.1 to R8.4. Assigning a Severe VSL for missing any one (or more) of R8.1 to R8.4 is like treating it like a binary requirement where in fact it can be graded according to how many of R4.1 to R4.4 are missed. Suggest to grade this.
R9	Should be expanded to make VSLs also dependent on the delay in documenting the modifications.
CIP-008-1	
R1	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R2	OK
CIP-009-1	
R1	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R2	Should be graded according to the delay in exercising the recovery plan.
R3	OK
R4	Should be graded according to the failure to meet the two conditions in R4: processes and procedures for the backup <u>and</u> storage of information required.
R5	Should be graded according to the delay in completing the annual testing.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Table 1

Summary of Comments on VSLs for Version 1 CIP Standards

Standard/ Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
CIP-002-2				
R1	None	None	None	This standard remains virtually the same as in Version 1 except some cosmetic changes in R4.
R1.1				
R1.2				
R1.2.1				
R1.2.2				
R1.2.3				
R1.2.4				
R1.2.5				
R1.2.6				
R1.2.7				
R2	None	None	None	
R3	None	None	None	
R3.1				
R3.2				
R3.2				
R4	Cosmetic	None	Cosmetic	Conforming changes
CIP-003-2				
R1	None			
R1.1	None			
R1.2	None			
R1.3	None			
R2	Cosmetic	None	Cosmetic	Conforming changes
R2.1	Cosmetic	None	Cosmetic	Conforming changes
R2.2	None			
R2.3	New	Lower	New	Binary VSL: Severe only.
R2.4	None	Lower	New	VRF Same as R2.3 in V1; Binary VSL: Severe only.
R3	None			
R3.1	None			
R3.2	Cosmetic	None	Cosmetic	Conforming changes
R3.3	None			
R4	None			
R4.1	None			
R4.2	None			
R4.3	None			
R5	None			
R5.1	None			
R5.2	None			
R5.3	None			
R6	None			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

CIP-004-2				
R1	Cosmetic	None	Cosmetic	Conforming changes
R2	Minor wording	None	Minor	Conforming changes
R2.1	Minor wording	None	Minor	Conforming changes
R2.2	None			
R2.2.1-				
R2.2.4				
R2.3	None			
R3	Minor wording	None	Minor	Conforming changes
R3.1	None			
R3.2	None			
R3.3	None			
R4	None			
R4.1	None			
R4.2	None			
CIP-005-2				
R1	None			
R1.1	None			
R1.2	None			
R1.3	None			
R1.4	None			
R1.5	Cosmetic	None	Cosmetic	Conforming changes
R1.6	None			
R2	None			
R2.1	None			
R2.2	None			
R2.3	Cosmetic	None	Cosmetic	Conforming changes
R2.4	None			
R2.5	None			
R2.6	None			
R3	None			
R3.1	None			
R3.2	None			
R4	None			
R4.1	None			
R4.2	None			
R4.3	None			
R4.4	None			
R4.5	None			
R5	Cosmetic		None	
R5.1	Cosmetic		None	
R5.2	None			
R5.3	Cosmetic		None	
CIP-006-2				

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R1	Minor wording	None	Minor	Conforming changes
R1.1	Minor wording	None	Minor	Conforming changes
R1.2	Cosmetic	None	Minor	Conforming changes
R1.3	None			
R1.4	Cosmetic	None	Minor	Conforming changes
R1.5	Cosmetic	None	Minor	Conforming changes
R1.6	Reworded	None	Minor	Conforming changes
R1.7	Minor wording	None	Minor	Conforming changes
R1.8	New	Lower	New	VRF same as R1.9 in V1; Binary VSL: Severe only.
R2	New	Medium	New	VSL has 4 levels whose assignments are dependent on meeting requirements in other CIP standards. This can be an issue.
R2.1	New	Medium	Removed	Rolled up to R2; but it has a VRF which by the general rule has to have a VSL!
R2.2	New	Medium	Removed	Rolled up to R2; but it has a VRF which by FERC's rule has to have a VSL!
R3	New	Medium	New	VRF is new; Binary VSL: Severe only.
R4	None (formerly R2)	Medium	Changed from VSLs for former R2).	VRF similar to R2 in V1; 3 VSLs from Moderate to Severe depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
R4.1-R4.4	Become bullets			See above comment.
R5	None (formerly R3)	Medium	Changed from VSLs for former R3)	VRF similar to R3 in V1; 3 VSLs from Moderate to Severe depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
R5.1-R5.2	Become bullets			
R6	None (Formerly R4)	Lower	Changed from VSLs for former R4)	VRF similar to R4 in V1; 4 VSLs depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
R6.1-R6.3	Become bullets			
R7	None (Formerly R5)	Lower	Similar to VSLs for	VRF similar to R5 in V1; Binary VSL: Severe only.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

			former R5)	
R8	Cosmetic (Formerly R6)	Medium	Similar to VSLs for former R6)	VRF similar to R6 in V1; 4 VSLs depending on which subrequirements the entity fails to comply.
R8.1	None	Medium	Removed	VRF similar to R6.1 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC’s rule has to have a VSL!
R8.2	Cosmetic	Lower	Removed	VRF similar to R6.2 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC’s rule has to have a VSL!
R8.3	None	Lower	Removed	VRF similar to R6.3 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC’s rule has to have a VSL!
CIP-007-2				
R1	Cosmetic	None	None	None
R1.1	None			
R1.2	None			
R1.3	None			
R2	Cosmetic	None	Minor	Conforming changes
R2.1	None	None	None	None
R2.2	None	None	None	None
R2.3	Minor wording	None	None	None
R3	Cosmetic	None	Minor	Conforming changes
R3.1	None	None	None	None
R3.2	Minor wording	None	None	None
R4	None			
R4.1	Minor wording	None	Minor	Conforming changes
R4.2	None			
R5	None			
R5.1	None			
R5.1.1	None			
R5.1.2	None			
R5.1.3	Cosmetic	None	Minor	Conforming changes
R5.2	None			
R5.2.1	None			
R5.2.2	None			
R5.2.3	None			
R5.3	None			
R5.3.1	None			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R5.3.2	None			
R5.3.3	None			
R6	None			
R6.1	None			
R6.2	None			
R6.3	None			
R6.4	None			
R6.5	None			
R7	Cosmetic	None	Minor	Conforming changes
R7.1	None			
R7.2	None			
R7.3	None			
R8	None			
R8.1	None			
R8.2	None			
R8.3	None			
R8.4	None			
R9	Cosmetic	None	Minor	Conforming changes
CIP-008-2				
R1	Wording changes	None	Minor	Conforming changes
R1.1	None			
R1.2	Minor wording			
R1.3	None			
R1.4	Cosmetic			
R1.5	None			
R1.6	Major changes			
R2	None			
CIP-009-2				
R1	None			
R1.1	None			
R1.2	None			
R2	None			
R3	Cosmetic	None	Minor	Conforming changes
R4	None			
R5	None			

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information (Complete this page for comments from one organization or individual.)		
Name:		
Organization:		
Telephone:		
E-mail:		
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	<input type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Group Comments (Complete this page if comments are from a group.)

Group Name: IRC Standards Review Committee

Lead Contact: Ben Li

Contact Organization: IESO

Contact Segment: 2

Contact Telephone: (647) 388-1498

Contact E-mail: ben@benli.ca

Additional Member Name	Additional Member Organization	Region*	Segment*
Charles Yeung	SPP	SPP	2
Patrick Brown	PJM	RFC	2
Lourdes Estrada-Saliner	CAISO	WECC	2
James Castle	NYISO	NPCC	2
Steve Myers	ERCOT	ERCOT	2
Matt Goldberg	ISO-NE	NPCC	2
Bill Phillips	MISO	MRO	2

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

*** If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Project 2008-06 Project Web site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-14 Project Web site:

http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Background Information:

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection — Issued January 18, 2008) approved eight version 1 Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with “Levels of Non-Compliance” instead of “Violation Severity Levels.” This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the ‘Levels of Non-compliance’ in the 83 regulatory-approved standards with ‘Violation Severity Levels’ which also required development of Violation Severity Levels for any new or revised standards.

The drafting team for Project 2008-14 Cyber Security Violation Severity Levels was tasked with drafting proposed VSLs to comply the FERC directives regarding the development of Violation Severity Levels for the version 1 cyber group of standards:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

The drafting team for Project 2008-14 is proposing a change to the scope of its SAR to include responsibility for developing the VSLs for Project 2008-06 and is seeking feedback on this proposal.

In a separate action, the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 was tasked with revising each of the version 1 cyber security standards to ensure that they conform to the latest version of the ERO Rules of Procedure, and to address the directives identified in FERC Order 706 and the issues identified by industry stakeholders. The SDT for Project 2008-06 Cyber Security Order 706 agreed that due to the extensive scope and varying complexity of the issues and the work involved in making these revisions to the cyber security standards, a multiphase approach for revising this set of standards was needed and was therefore adopted.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Phase 1 of Project 2008-06 Cyber Security Order 706 includes the necessary modifications to the version 1 cyber security standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706 and 706A. As part of the initial phase of this project, the SDT has posted the version 2 CIP-002-2 through CIP-009-2 standards for industry comment and pre-ballot review absent the version 2 VRFs and VSLs.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are now posting proposed VSLs for industry comment and the team working on the version 2 standards is also posting proposed VRFs.

- The drafting team for Project 2008-14 Cyber Security Violation Severity Levels is posting proposed VSLs for the version 1 CIP-002-1 thru CIP-009-1 standards, and a proposed revision to its SAR.
- The standard drafting team for Project 2008-06 Cyber Security Order 706 is posting **both** proposed VRFs and proposed VSLs for the version 2 CIP-002-2 thru CIP-009-2 standards.

The version 1 VSLs are a comprehensive set of VSLs for every requirement of the version 1 CIP-002-1 thru CIP-009-1 standards as directed in FERC Order 706. However, the version 2 VSLs only include proposed modifications to the version 1 VSLs to be consistent with the changes proposed in the version 2 CIP-002-2 thru CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. The team is only posting version 2 VRFs for the two standards (CIP-003-2 and CIP-006-2) where the team added new VRFs, and for these two standards, the team is only seeking comment on the 15 version 2 VRFs that are “new”. These “new” VRFs are clearly identified in the posted document.

With this comment form, stakeholders are being asked to comment on four separate items:

- (1) the complete set of version 1 VSLs
- (2) the incremental changes to the version 1 VSLs proposed to create the version 2 VSLs
 - All comments submitted on the version 1 VSLs will automatically apply to the version 2 VSLs and therefore need not be repeated relative to the version 2 VSLs. Any changes made to the version 1 VSLs as a result of comments received from industry will automatically be applied to the version 2 VSLs.
- (3) the 15 “new” version 2 VRFs proposed for CIP-003-2 and CIP-006-2
- (4) the acceptability of the proposal to have one drafting team develop all the VSLs for both the version 1 and later versions of the CIP standards

The version 2 VRFs, and version 1 and version 2 VSLs in the accompanying documents are organized numerically by standard and requirement number.

The drafting teams for both Project 2008-06 Cyber Security Order 706 and Project 2008-14 Cyber Security Violation Severity Levels are requesting industry comments on the proposed VRFs and VSLs. Accordingly, we request that you complete and submit this form to Lauren Koller by **April 20, 2009**.

***Note:**

If you need to add a row to the table below please select Table from the above toolbar than Insert “Row Above” or “Row Below”

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

- 2. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Incremental Lower VSL Language	Alternate Incremental Moderate VSL Language	Alternate Incremental High VSL Language	Alternate Incremental Severe VSL Language

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

3. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.

Agree

Disagree

Comments:

4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

We did not fill out any of the tables above since we feel that it would more meaningful to offer the following high-level comments for the SDT's consideration as it revises the VSLs. Table 1, attached, provides a summary assessment of each of the VSLs proposed for the Version 1 CIP standards. Please also refer to Table 1 for the specific examples cited in the comments below.

1. The existing standard structure and quality do not lend themselves to the development of appropriate and effective VSLs. There are still VRFs assigned to the subrequirements which according to FERC need to have VSLs. This makes it very convoluted to develop the main requirement's VSLs which to a good extent depend on the failure to comply with any of the subrequirements which may have multiple levels of VSL themselves. Further, a key problem arises when the main requirement is assign a binary VSL (Severe) while its subrequirements are graded. Often, the main requirement and some of its subrequirements are of similar nature. Hence, a violation of that similar natured requirement will subject an entity to double penalties.

This is the problem we cited in the NERC's filing on the 322 VSL sets in the beginning of the year. The industry will need to continue to deal with this misfit issue until the requirements themselves are revamped and restructured.

The remaining comments provided in the Comment Form are developed ignoring this issue, i.e., the way the standards are written not how they should be written, and deal with the VSLs proposed for each main and subrequirement and look for consistency among the VSLs assigned to the requirements.

2. Some VSLs can be graded, but they are treated as binary. Some examples are (not exhaustive): R1 and R1.2 in CIP-002-1, R2 and R4.2 in CIP-003-1, R2.3 and R3.2 in CIP-007-1. Suggestions to grade these requirements and other such requirements are provided in Table 1.
3. Some requirements are assessed complete failure (Severe) if any one of the subrequirements is not met. This is clearly unacceptable since if the argument is that failing one of them essentially fails the bulk of the intent of the main requirement, then what about failing one of the remaining subrequirements? Do they all rise up to the level that failing any one would mean failing the bulk of the intent of the main requirements?

Examples are: R4 in CIP-005-1, R8 in CIP-007. Detailed suggestions to make this change grade are provided in Table 1.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

4. Some subrequirements' violations are "rolled-up" to determine the main requirements' VSLs, which is the proper way. However, this approach is not consistently applied and in some cases where it is applied, there are no VSLs proposed for the subrequirements despite they are assigned VRFs. This is not consistent with the approach applied elsewhere in the CIP standards or the FERC directives. Examples are: R2, R3, R4 and R6 of CIP-006-1, R1 and R7 in CIP-007-1. A consistent approach needs to be applied to all requirements.
5. For requirements of similar nature, some are graded while others are not. This is inconsistent. Some examples re: R2.1 to R2.3 compared to R3.1 to R3.3 in CIP-003-1.
6. Some requirements have listed under it, or included in the sentence, a number of conditions to be met yet the VSLs make no mention of these conditions. Examples are: R1 of CIP-004-1 and R1 of CIP-006-1.

5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?

- Agree
 Disagree

Comments:

6. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

Table 2, attached provides a summary assessment of the VRFs and VSLs for the Version 2 CIP standards. Examples cited in the comments below can be found in table 2.

Similar problems as identified for the Version 1 CIP standards VSLs are also identified among the VSLs for the Version 2 CIP standards.

Table 1
Summary of Comments on VSLs for Version 1 CIP Standards

Standard/ Requirement	Assessment/Comment
CIP-002-1	
R1	R1 is poorly structured. Comment on VSL can only be made based on how it's written, not how it should be written. VSL for R1 is binary, which it shouldn't be. It is a good example of how inappropriate to have a binary requirement while its subrequirements' VSLs are a mixture of binary and graded.
R1.1	Graded, but not based on the failure of its subrequirements.
R1.2 R1.2.1 – R1.2.7	VSL for R1.2 is binary, which could be graded depending on the failure to meet any of its subrequirements.
R2	OK, but the last part “even if such list is null” seems irrelevant.
R3	The VSLs for R3 should be graded to also cover the Low and Moderate columns since it has subrequirements R3.1 to R3.3 all of which need to be met fully comply with R3. Further, the last part “even if such list is null” under the Severe condition seems irrelevant.
R3.1	Binary; OK.
R3.2	Ditto
R3.3	Ditto
R4	OK.
CIP-003-1	
R1	The VSLs are determined w/o regard to any of the subrequirements, which they should.
R1.1	Binary: OK, and hence should form the basis for determining the VSL for R1.
R1.2	Ditto
R1.3	Not binary. In itself OK. These VSLs can also form the basis for determining the VSL for R1.
R2	The VSL should be graded according to how many of R2.1 to R2.3 are missed.
R2.1	OK as a condition to determine R2, but itself can be graded according to which elements are missing.
R2.2	OK as a condition to determine R2, but itself can be graded according to how late the document is issued.
R2.3	OK as a condition to determine R2, but itself can be graded since there are two conditions in this subrequirement.
R3	It doesn't make sense that the Low and Moderate entries are assigned N/A when the VSLs can be further graded to capture the conditions where the responsible entity fails to meet any of R3.1 to R3.3.
R3.1	The VSLs for this and the other two subrequirements seem OK, but it illustrates the inconsistent approach between R2 and R3. The VSLs for R2's subrequirements should be graded in a similar fashion.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R3.2	See above comment.
R3.3	See above comment.
R4	OK, given the nature of the main and subrequirements and the fact that separate VRFs are assigned to them. A more appropriate approach would be to grade R4's VSLs according to the extent to which the responsible entity fails to meet its subrequirements.
R4.1	The VSL starts off at the High level for missing one of the elements. This should be Low. Missing 2 a Moderate, 3 a High, etc.
R4.2	The VSL could be graded according to the percentage of information that is not classified.
R4.3	OK.
R5	OK given the way the main and subrequirements are written and the fact that separate VRFs are assigned to them. A more appropriate approach would be to grade R5's VSLs according to the extent to which the responsible entity fails to meet the subrequirements.
R5.1	The VSL for R5.1 should be graded according to the extent of failure to meet R5.1.1 and R5.1.2 since they are the conditions for fully meeting R5.1.
R5.1.1	Should be graded since there are a number of elements in this subrequirement.
R5.1.2	Should be graded according to the delay in verifying the information.
R5.2	Should be graded according to the delay in completing the review.
R5.3	Should be graded according to the delay in assessing and documenting the processes.
R6	OK.
CIP-004-1	
R1	OK, but could be improved to consider inclusion of the bulleted elements.
R2	OK given the current structure and assignment of VRFs to R2 and its subrequirements.
R2.1	OK
R2.2	Could be improved to stipulate conditions for Low and Moderate since the requirement itself contains several conditions: "...policies, access controls, and procedures". None of them are covered in the High and Severe VSLs.
R2.3	OK.
R3	OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R3.1	OK
R3.2	OK
R3.3	OK
R4	OK given the current structure and assignment of VRFs to R4 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R4.1	OK
R4.2	OK
CIP-005-1	

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R1	OK given the current structure and assignment of VRFs to R1 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R1.1	OK
R1.2	OK
R1.3	OK
R1.4	OK
R1.5	OK
R1.6	OK
R2	OK given the current structure and assignment of VRFs to R2 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R2.1	OK
R2.2	OK
R2.3	OK
R2.4	OK
R2.5	OK
R2.6	OK
R3	OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R3.1	OK
R3.2	OK
R4	OK for the conditions that are independent of R4.1 to R4.4. Assigning a Severe VSL for missing any one (or more) of R4.1 to R4.4 is like treating it a like binary requirement where in fact it can be graded according to how many of R4.1 to R4.4 are missed. Suggest to grade this.
R5	OK given the current structure and assignment of VRFs to R5 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R5.1	OK
R5.2	OK
R5.3	Should be graded according to the number of days that the log was maintained.
CIP-006-1	
R1	The VSLs for R1 should be determined according to the extent of failure to meet any of its subrequirements this requirement, as it is so clearly indicated in R1 that the plan shall address, at a minimum, the subrequirements that follow.
R1.1	O.
R1.2	OK
R1.3	OK as a condition to determine the VSL for R1 but since it is not, the VSLs for R1.3 should be graded according to which element among “processes, tools, and procedures” is missing.
R1.4	OK
R1.5	OK

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R1.6	OK
R1.7	OK
R1.8	OK
R1.9	OK
R2	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R3	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R4	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R5	Should be graded according to the number of days that the log was maintained.
R6	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
CIP-007-1	
R1	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R2	OK given the current structure and assignment of VRFs to R2 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R2.1	OK.
R2.2	OK
R2.3	Should be graded according to the number or % of cases that the responsible entity failed to document compensated measure(s) for those unused ports and services cannot be disabled.
R3	OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R3.1	OK
R3.2	Should be graded according to the number or % of cases that the responsible entity failed to document the implementation of security patches and/or failed to document compensated measure(s) for those patches that are not installed.
R4	OK given the current structure and assignment of VRFs to R4 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R4.1	Should be graded according to the number or % of cases that the responsible entity failed to meet either of the two conditions stipulated in this subrequirements.
R4.2	OK
R5	OK given the current structure and assignment of VRFs to R5 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R5.1	Should be graded according to which of R5.1.1 to R5.1.2 are missed since they are the required elements in the policy.
R5.1.1	OK by itself but it should get rolled up to the determination of VSLs for R5.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R5.1.2	OK by itself but it should get rolled up to the determination of VSLs for R5.
R5.1.3	Binary is OK if it was rolled up to the determination of VSLs for R5. Otherwise, the VSLs should be graded according to the delay in completing the annual review.
R5.2	Disagree with the binary VSL since to fully meet the intent of R5.2, all of its subrequirements must be complied with. The VSLs for R5.2 should be graded according to the extent of failing to meet any of its subrequirements.
R5.2.1	OK
R5.2.2	Should be graded according to the number or % of the individuals that the responsible entity failed to identify.
R5.2.3	OK
R5.3	OK
R6	OK given the current structure and assignment of VRFs to R6 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.
R6.1	OK
R6.2	OK
R6.3	OK
R6.4	OK
R6.5	Should be graded according to the number or % of the logged cases that the responsible entity failed to review and provided records documenting the review.
R7	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R8	OK for the conditions that are independent of R8.1 to R8.4. Assigning a Severe VSL for missing any one (or more) of R8.1 to R8.4 is like treating it like a binary requirement where in fact it can be graded according to how many of R4.1 to R4.4 are missed. Suggest to grade this.
R9	Should be expanded to make VSLs also dependent on the delay in documenting the modifications.
CIP-008-1	
R1	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R2	OK
CIP-009-1	
R1	OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!
R2	Should be graded according to the delay in exercising the recovery plan.
R3	OK
R4	Should be graded according to the failure to meet the two conditions in R4: processes and procedures for the backup <u>and</u> storage of information required.
R5	Should be graded according to the delay in completing the annual testing.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

Table 2

Summary of Comments on VSLs for Version 1 CIP Standards

Standard/ Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
CIP-002-2				
R1	None	None	None	This standard remains virtually the same as in Version 1 except some cosmetic changes in R4.
R1.1				
R1.2				
R1.2.1				
R1.2.2				
R1.2.3				
R1.2.4				
R1.2.5				
R1.2.6				
R1.2.7				
R2	None	None	None	
R3	None	None	None	
R3.1				
R3.2				
R3.2				
R4	Cosmetic	None	Cosmetic	Conforming changes
CIP-003-2				
R1	None			
R1.1	None			
R1.2	None			
R1.3	None			
R2	Cosmetic	None	Cosmetic	Conforming changes
R2.1	Cosmetic	None	Cosmetic	Conforming changes
R2.2	None			
R2.3	New	Lower	New	Binary VSL: Severe only.
R2.4	None	Lower	New	VRF Same as R2.3 in V1; Binary VSL: Severe only.
R3	None			
R3.1	None			
R3.2	Cosmetic	None	Cosmetic	Conforming changes
R3.3	None			
R4	None			
R4.1	None			
R4.2	None			
R4.3	None			
R5	None			
R5.1	None			
R5.2	None			
R5.3	None			
R6	None			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

CIP-004-2				
R1	Cosmetic	None	Cosmetic	Conforming changes
R2	Minor wording	None	Minor	Conforming changes
R2.1	Minor wording	None	Minor	Conforming changes
R2.2	None			
R2.2.1-				
R2.2.4				
R2.3	None			
R3	Minor wording	None	Minor	Conforming changes
R3.1	None			
R3.2	None			
R3.3	None			
R4	None			
R4.1	None			
R4.2	None			
CIP-005-2				
R1	None			
R1.1	None			
R1.2	None			
R1.3	None			
R1.4	None			
R1.5	Cosmetic	None	Cosmetic	Conforming changes
R1.6	None			
R2	None			
R2.1	None			
R2.2	None			
R2.3	Cosmetic	None	Cosmetic	Conforming changes
R2.4	None			
R2.5	None			
R2.6	None			
R3	None			
R3.1	None			
R3.2	None			
R4	None			
R4.1	None			
R4.2	None			
R4.3	None			
R4.4	None			
R4.5	None			
R5	Cosmetic		None	
R5.1	Cosmetic		None	
R5.2	None			
R5.3	Cosmetic		None	
CIP-006-2				

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R1	Minor wording	None	Minor	Conforming changes
R1.1	Minor wording	None	Minor	Conforming changes
R1.2	Cosmetic	None	Minor	Conforming changes
R1.3	None			
R1.4	Cosmetic	None	Minor	Conforming changes
R1.5	Cosmetic	None	Minor	Conforming changes
R1.6	Reworded	None	Minor	Conforming changes
R1.7	Minor wording	None	Minor	Conforming changes
R1.8	New	Lower	New	VRF same as R1.9 in V1; Binary VSL: Severe only.
R2	New	Medium	New	VSL has 4 levels whose assignments are dependent on meeting requirements in other CIP standards. This can be an issue.
R2.1	New	Medium	Removed	Rolled up to R2; but it has a VRF which by the general rule has to have a VSL!
R2.2	New	Medium	Removed	Rolled up to R2; but it has a VRF which by FERC's rule has to have a VSL!
R3	New	Medium	New	VRF is new; Binary VSL: Severe only.
R4	None (formerly R2)	Medium	Changed from VSLs for former R2).	VRF similar to R2 in V1; 3 VSLs from Moderate to Severe depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
R4.1-R4.4	Become bullets			See above comment.
R5	None (formerly R3)	Medium	Changed from VSLs for former R3)	VRF similar to R3 in V1; 3 VSLs from Moderate to Severe depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
R5.1-R5.2	Become bullets			
R6	None (Formerly R4)	Lower	Changed from VSLs for former R4)	VRF similar to R4 in V1; 4 VSLs depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
R6.1-R6.3	Become bullets			
R7	None (Formerly R5)	Lower	Similar to VSLs for	VRF similar to R5 in V1; Binary VSL: Severe only.

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

			former R5)	
R8	Cosmetic (Formerly R6)	Medium	Similar to VSLs for former R6)	VRF similar to R6 in V1; 4 VSLs depending on which subrequirements the entity fails to comply.
R8.1	None	Medium	Removed	VRF similar to R6.1 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC's rule has to have a VSL!
R8.2	Cosmetic	Lower	Removed	VRF similar to R6.2 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC's rule has to have a VSL!
R8.3	None	Lower	Removed	VRF similar to R6.3 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC's rule has to have a VSL!
CIP-007-2				
R1	Cosmetic	None	None	None
R1.1	None			
R1.2	None			
R1.3	None			
R2	Cosmetic	None	Minor	Conforming changes
R2.1	None	None	None	None
R2.2	None	None	None	None
R2.3	Minor wording	None	None	None
R3	Cosmetic	None	Minor	Conforming changes
R3.1	None	None	None	None
R3.2	Minor wording	None	None	None
R4	None			
R4.1	Minor wording	None	Minor	Conforming changes
R4.2	None			
R5	None			
R5.1	None			
R5.1.1	None			
R5.1.2	None			
R5.1.3	Cosmetic	None	Minor	Conforming changes
R5.2	None			
R5.2.1	None			
R5.2.2	None			
R5.2.3	None			
R5.3	None			
R5.3.1	None			

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

R5.3.2	None			
R5.3.3	None			
R6	None			
R6.1	None			
R6.2	None			
R6.3	None			
R6.4	None			
R6.5	None			
R7	Cosmetic	None	Minor	Conforming changes
R7.1	None			
R7.2	None			
R7.3	None			
R8	None			
R8.1	None			
R8.2	None			
R8.3	None			
R8.4	None			
R9	Cosmetic	None	Minor	Conforming changes
CIP-008-2				
R1	Wording changes	None	Minor	Conforming changes
R1.1	None			
R1.2	Minor wording			
R1.3	None			
R1.4	Cosmetic			
R1.5	None			
R1.6	Major changes			
R2	None			
CIP-009-2				
R1	None			
R1.1	None			
R1.2	None			
R2	None			
R3	Cosmetic	None	Minor	Conforming changes
R4	None			
R5	None			

Official Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Please use this form to submit comments on the proposed Violation Severity Levels (VSLs) for Versions 1 and 2 of the CIP-002 through CIP-009 standards, proposed Violation Risk Factors (VRFs) for Version 2 of CIP-003 and CIP-006, and a proposed change to the SAR for Project 2008-14.

Comments must be submitted by April 20, 2009. You may submit the completed form by e-mail to sarcomm@nerc.net with the words "Cyber Security VRF and VSL Comment Form" in the subject line. If you have any questions on the subject information please contact Al Calafiore at Al.Calafiore@nerc.net or David Taylor at David.Taylor@nerc.net.

Individual Commenter Information		
(Complete this page for comments from one organization or individual.)		
Name:	Michael P Mertz	
Organization:	Southern California Edison Company	
Telephone:	626-543-6104	
E-mail:	michael.mertz@sce.com	
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input checked="" type="checkbox"/>	1 — Transmission Owners
<input type="checkbox"/> FRCC	<input type="checkbox"/>	2 — RTOs and ISOs
<input type="checkbox"/> MRO	<input checked="" type="checkbox"/>	3 — Load-serving Entities
<input type="checkbox"/> NPCC	<input type="checkbox"/>	4 — Transmission-dependent Utilities
<input type="checkbox"/> RFC	<input checked="" type="checkbox"/>	5 — Electric Generators
<input type="checkbox"/> SERC	<input checked="" type="checkbox"/>	6 — Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> SPP	<input type="checkbox"/>	7 — Large Electricity End Users
<input checked="" type="checkbox"/> WECC	<input type="checkbox"/>	8 — Small Electricity End Users
<input type="checkbox"/> NA – Not Applicable	<input type="checkbox"/>	9 — Federal, State, Provincial Regulatory or other Government Entities
	<input type="checkbox"/>	10 — Regional Reliability Organizations and Regional Entities

Comment Form for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs) and Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VRFs and VSLs)

You do not have to answer all questions. Enter All Comments in Simple Text Format.

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.**

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
CIP-002-1	R1			The responsible entity has documented a risk-based assessment methodology but has not applied it to identify its Critical Assets as specified in R1.	The responsible entity has documented a risk-based assessment methodology but has not applied it to identify its Critical Assets as specified in R1.
	R1.1	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes evaluation criteria but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that did not include procedures and evaluation criteria.
	R3.1			A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.	Two or more Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
	R3.2			A Cyber Asset essential to the operation of the Critical Asset was identified that	Two or more Cyber Asset essential to the operation of the Critical Asset was

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
				met the criteria in this requirement but was not included in the Critical Cyber Asset List.	identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
	R3.3			A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.	Two or more Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
	R4	N/A	N/A	<p>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of the list of Critical Assets (even if such list is null)</p> <p>or</p> <p>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of the list of the list of Critical Cyber Assets</p>	
CIP-003-1	R1.1	The Responsible Entity's cyber security policy does address all the requirements in	The Responsible Entity's cyber security policy does not address all the requirements in Standards	N/A	N/A

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
		Standards CIP-002 through CIP-009, however, it does not include provision for emergency situations.	CIP-002 through CIP-009, nor does it include provision for emergency situations.		
	R1.2			The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
	R2.1		The senior manager is not identified by one of the following; name, title, business phone, business address, and date of designation.	The senior manager is not identified by name, title, business phone, business address, and date of designation.	The senior manager is not identified by name, title, business phone, business address, and date of designation.
	R2.2			Changes to the senior manager were documented but not within thirty calendar days of the effective date.	Changes to the senior manager were not documented within thirty calendar days of the effective date.
	R2.3			The senior manager or delegate(s) authorized exception to the Cyber Security Policy but did not document exception within thirty days.	

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
	R3.2			<p>The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include an explanation as to why the exception is necessary</p> <p>OR</p> <p>The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but the exception did not include compensating measures or a statement accepting risk.</p>	<p>The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include an explanation as to why the exception is necessary, nor did it include any compensating measures or a statement accepting risk.</p>
	R4			<p>The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.</p>	
	R5			<p>The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.</p>	

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
	R5.1			The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	
	R5.1.1		The Responsible Entity did identify the personnel by name, title, business phone but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name, title, business phone nor the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name, title, business phone nor the information for which they are responsible for authorizing access.
	R5.1.2			The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
	R5.2			The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
	R5.3			The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-004-1	R1		The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. And did not provide security awareness reinforcement on at least a quarterly basis.		
	R2		The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets and did not review the training program on an annual basis.		

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
	R2.2		The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
	R2.3		The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.
	R3			The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in thirty (30) days of such personnel being granted such access.	
CIP-005-1	R1	The Responsible Entity did not document one or more access points to the electronic security perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document	The Responsible Entity did not ensure that one or more Critical Cyber Asset resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document one or more Electronic

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
				one or more Electronic Security Perimeter(s).	Security Perimeter(s)
	R1.1			Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
	R1.2			For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.	For more than two (2) dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
	R1.3			At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
	R1.4	One or more non-critical	One or more non-critical	One or more non-critical	One or more non-critical

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
		Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.	Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
	R1.6		The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
	R2.3		The Responsible Entity has a procedure but not maintained for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not document nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not document, implement, nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
	R2.4				Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
	R2.6		Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.		
	R3.1	Where technically feasible, the Responsible Entity implemented but did not documented electronic or manual processes monitoring and logging at less than 5% of the access points to dial-up devices.			

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
	R5.3			The responsible Entity did not retain electronic access logs for at least 90 calendar days.	The responsible Entity did not retain electronic access logs for at least 90 calendar days.
CIP-006-1	R1.1			<p>The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.</p> <p>OR</p> <p>Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed nor documented alternative measures to control physical access to the Critical Cyber Assets.</p>	

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
	R1.7		The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration but the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.
	R5			The Responsible Entity did not retain electronic access logs for at least ninety calendar days.	The Responsible Entity did not retain electronic access logs for at least ninety calendar days.
CIP-007-1	R1				The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
					<p>AND</p> <p>The Responsible Entity did not document the test results as required in R1.3.</p>
	R2	The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A	N/A
	R2.2	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
	R3.2				The Responsible Entity did not document the implementation of applicable security patches as required in R3.

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
					<p>OR</p> <p>Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.</p>
	R4.1			<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.</p>	<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.</p>
	R4.2	The Responsible Entity documented and	The Responsible Entity implemented but did not document a process,		

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
		implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing and installing of the signatures.	including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”		
	R5		The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implemented technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
	R5.1			The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.
	R5.1.1	At least one user account but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	5 % or more but less than 10% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	10 % or more but less than 15% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	15 % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
	R5.2			The Responsible Entity implemented but did not document a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	The Responsible Entity implemented but did not document a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
	R5.2.2	The Responsible Entity did not identify <5% all individuals with access to shared accounts.	The Responsible Entity did not identify between 5-10% all individuals with access to shared accounts.	The Responsible Entity did not identify between 10-15% all individuals with access to shared accounts.	The Responsible Entity did not identify >15% individuals with access to shared accounts.
	R5.3	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.		
	R6.5			The Responsible Entity reviewed but not documented logs of system events related to cyber security nor maintain records documenting review of logs.	The Responsible Entity reviewed but not documented logs of system events related to cyber security nor maintain records documenting review of logs.
	R9		The Responsible Entity did not review and update the	The Responsible Entity did	The Responsible Entity

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
			documentation specified in Standard CIP-007 at least annually or the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.	did not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.
CIP-009-1	R1	The Responsible Entity has documented but not annually reviewed recovery plan(s) for Critical Cyber Assets.	The Responsible Entity has created recovery plan(s) for Critical Cyber Assets but did not address one of the requirements CIP-009-1 R1.1 and R1.2.	The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-1 R1.1 and R1.2.	The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-1 R1.1 and R1.2.
	R2			The Responsible Entity's recovery plan(s) have not been exercised at least annually.	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-003-2	R2.1			The senior manager is not identified by name, title, and date of designation.	The senior manager is not identified by name, title, business phone, business address, and date of designation.
	R2.3			A senior manager's delegate is not identified by name, title, and date of designation; or changes to the delegated authority are not documented within	The document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
				thirty calendar days of the effective date.	by the senior manager.
CIP-004-2	R3				<p>The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access.</p> <p>OR</p> <p>The Responsible Entity did not conduct the personnel risk assessment pursuant to that program prior to personnel being granted such access except in specified circumstances such as an emergency.</p>
CIP-005-2	R2.3				The Responsible Entity did not document, implement, nor maintain a procedure for securing dial-up access to the

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
					Electronic Security Perimeter(s) where applicable.
CIP-006-2	R1.1				<p>The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.</p> <p>OR</p> <p>Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed nor documented alternative measures to control physical access to Cyber Assets.</p>
	R1.7		The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within thirty calendar days of the completion of a physical	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within thirty calendar days of the completion of a

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
			reconfiguration but the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.	security system redesign or reconfiguration.	physical security system redesign or reconfiguration.
	R1.8			The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
	R3				A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
	R7			The Responsible Entity did not retain electronic access logs in accordance with the requirements of Standard CIP-008-2.	The Responsible Entity did not retain electronic access logs in accordance with the requirements of Standard CIP-008-2.
CIP-007-2	R4.1			The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
				<p>perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.</p>	<p>perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.</p>
	R5.1.3			<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.</p>	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.</p>
	R9		<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>The Responsible Entity did not document changes</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the</p>

Standard Number	Requirement Number	Alternate Lower VSL Language	Alternate Moderate VSL Language	Alternate High VSL Language	Alternate Severe VSL Language
			resulting from modifications to the systems or controls within thirty calendar days of the change being completed.		change being completed.

2. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.

Agree

Disagree

Comments:

3. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Comments:

1. The VSLs drafted for CIP-002-1 through CIP-009-1 double-count violations for Requirements and Sub-Requirements, for example, a violation to CIP-003-1 R2 will inherit violations to R2.1, R2.2 or R2.3.
2. CIP-007 R2.2 and R2.1 are redundant, and represent the same violation.
3. When viewed as a whole, the ratings are inconsistent from one requirement to the next and do not appear to consider the criticality of the item in question. For instance, failure to annually review recovery plans for CCAs is rated as Moderate, while failure to document changes to the senior manager's phone number within 30 days is rated as Severe. Variations in like-measurements occur throughout. For instance, missing elements for one document will be rated as Moderate, another as Severe, and yet another with a full spectrum based on the percentage of completion. In most cases, the type of document is similar with no significant variance in risk.

4. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?

Agree

Disagree

Comments: The senior manager is not identified by name, title, business phone, business address, and date

- 5. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.**

Comments:

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

The Cyber Security Order 706 Standard Drafting Team and Cyber Security Violation Severity Levels Drafting Teams thank all commenters who submitted comments on the CIP Version 2 VSLs and VRFs. The Version 2 VRFs and VSLs were posted for a 30-day public comment period from March 16, 2009 through April 20, 2009. Stakeholders were asked to provide feedback through a Word document Comment Form. There were 12 sets of comments, including comments from more than 60 different people from over 45 companies representing 7 of the 10 Industry Segments as shown in the table on the following pages.

While the comment form addressed VSLs for the Version 1 Cyber Security Standards and the SAR for that project as well as the VSLs and VRFs for the Version 2 Cyber Security Standards, this report addresses only the VRFs and VSLs for Version 2 Cyber Security Standards. Comments related to the Version 1 Cyber Security VSLs were addressed in a separate report.

For this report, stakeholder comments were sorted so that it is easier to see all related comments. All comments have been posted in their original format at the following site:

Project 2008-14 Cyber Security Violation Severity Levels Drafting Team:
http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html

Based on stakeholder comments, the drafting team did make some changes to some of the sets of VSLs for CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, and CIP-006-2. No changes were made to VSLs for CIP-007-2, CIP-008-2 or for CIP-009-2. Most changes were either clarifying or format changes. In some cases, stakeholders identified additional descriptions of noncompliant performance that could be used to add more options to the already proposed VSLs – and where the proposed VSLs met the definitions for the proposed VSL category, the proposed VSLs were adopted.

Some stakeholders are opposed to setting noncompliance with a binary requirement or subrequirement as a “Severe” VSL. If an entity is totally noncompliant with a requirement, then this meets the criteria for a “Severe” VSL.

Some stakeholders commented that the drafting team should have developed a single set of VSLs for a requirement and its associated subrequirements. The drafting team agrees that having a single set of VSLs for each requirement, in its entirety, is preferable, however, in accordance with the directives in FERC's VSL Order, the drafting team has assigned a set of VSLs to each requirement and each subrequirement that has a VRF. Note that there are a few exceptions where the drafting team felt it could reasonably use a “roll-up” approach to VSLs, it did so. Where both the requirement and the subrequirement have sets of VSLs, the team has taken care to develop VSLs that should not result in double jeopardy.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.¹

¹ The appeals process is in the Reliability Standards Development Procedures:
<http://www.nerc.com/standards/newstandardsprocess.html>.

Index to Questions, Comments, and Responses

1. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision. 8
2. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why..... 14
3. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here. 15

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

The Industry Segments are:

- 1 — Transmission Owners
- 2 — RTOs, ISOs
- 3 — Load-serving Entities
- 4 — Transmission-dependent Utilities
- 5 — Electric Generators
- 6 — Electricity Brokers, Aggregators, and Marketers
- 7 — Large Electricity End Users
- 8 — Small Electricity End Users
- 9 — Federal, State, Provincial Regulatory or other Government Entities
- 10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment										
				1	2	3	4	5	6	7	8	9	10	
1.	Group 1	Ben Li	IRC Standards Review Committee		X									
2.	Group 1	Charles Yeung	SPP		X									
3.	Group 1	Patrick Brown	PJM		X									
4.	Group 1	Lourdes Estrada-Saliner	CAISO		X									
5.	Group 1	James Castle	NYISO		X									
6.	Group 1	Steve Myers	ERCOT		X									
7.	Group 1	Matt Goldberg	ISO-NE		X									
8.	Group 1	Bill Phillips	MISO		X									
9.	Individual	Chris Scanlon	Exelon	X										
10.	Individual	Dan Rochester	IESO		X									

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

		Commenter	Organization	Industry Segment										
				1	2	3	4	5	6	7	8	9	10	
11.	Group 2	Denise Koehn	Bonneville Power Administration	X										
12.	Group 2	Huy Ngo	Control Cntr HW Design & Maint	X										
13.	Group 2	Allen Chan	General Counsel	X		X		X	X					
14.	Group 2	Robin Chung	Generation Support			X		X	X					
15.	Group 2	Sheree Chambers	Power Scheduling Coordination			X		X	X					
16.	Group 2	Tina Weber	Power Scheduling Coordination			X		X	X					
17.	Group 2	Pete Jeter	Security & Emergency Response	X		X		X	X					
18.	Group 2	Erik Smith	Security & Emergency Response	X		X		X	X					
19.	Group 2	Dick Winters	Substation Operations	X										
20.	Group 2	Curt Wilkins	Transmission System Operations	X										
21.	Group 2	Kelly Hazelton	Transmission System Operations	X										
22.	Group 2	Jim Domschot	Transmission Work Planning and Evaluation	X										
23.	Group 2	Jim Jackson	Transmission Work Planning and Evaluation	X										
24.	Group 2	Kevin Dorning	Tx PSC Technical Services	X										
25.	Individual	Greg Rowland	Duke Energy	X		X		X	X					
26.	Group 3	Guy Zito	Northeast Power Coordinating Council											X
27.	Group 3	Ralph Rufrano	New York Power Authority					X						
28.	Group 3	Rick White	Northeast Utilities	X										

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

		Commenter	Organization	Industry Segment										
				1	2	3	4	5	6	7	8	9	10	
29.	Group 3	Chris de Graffenried	Consolidated Edison Com. Of New York, Inc.	X										
30.	Group 3	David Kiguel	Hydro One Networks Inc.	X										
31.	Group 3	Randy MacDonald	New Brunswick System Operator		X									
32.	Group 3	Roger Champagne	Hydro-Quebec TransEnergie		X									
33.	Group 3	Tony Elacqua	New York Independent System Operator		X									
34.	Group 3	Manny Couto	National Grid	X										
35.	Group 3	Kathleen Goodman	ISO - New England		X									
36.	Group 3	Brian Evans-Mongeon	Utility Services, LLC						X					
37.	Group 3	Mike Garton	Dominion Resources Services					X						
38.	Group 3	Chris Orzel	FPL/NextEra					X						
39.	Group 3	Sylvain Clermont	Hydro-Quebec TransEnergie	X										
40.	Group 3	Kurtis Chong	Independent Electricity System Operator		X									
41.	Group 3	Lee Pedowicz	Northeast Power Coordinating Council											X
42.	Group 3	Gerry Dunbar	Northeast Power Coordinating Council											X
43.	Group 3	Mike Gildea	Constellation Energy						X					
44.	Group 3	Michael Schiavone	National Grid	X										
45.	Group 3	Brian Hogue	Northeast Power Coordinating Council											X

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

		Commenter	Organization	Industry Segment																
				1	2	3	4	5	6	7	8	9	10							
46.	Group 4	Michael Brytowski	MRO NERC Standards Review Subcommittee																	X
47.	Group 4	Carol Gerou	MP	X		X		X	X											
48.	Group 4	Neal Balu	WPS			X	X	X	X											
49.	Group 4	Terry Bilke	MISO		X															
50.	Group 4	Joe DePoorter	MGE			X	X	X	X											
51.	Group 4	Ken Goldsmith	ALTW				X													
52.	Group 4	Jim Haigh	WAPA	X						X										
53.	Group 4	Terry Harbour	MEC	X		X		X	X											
54.	Group 4	Joseph Knight	GRE	X		X		X	X											
55.	Group 4	Scott Nickels	RPU			X	X	X	X											
56.	Group 4	Dave Rudolph	BEPC	X		X		X	X											
57.	Group 4	Eric Ruskamp	LES	X		X		X	X											
58.	Group 4	Pam Sordet	XCEL	X		X		X	X											
59.	Individual	Michael J. Sonnelitter	NextEra Energy Resources, LLC					X												
60.	Individual	Michael Gammon	Kansas City Power & Light	X		X		X	X											
61.	Individual	Paul McClay	Tampa Electric Company	X		X		X	X											
62.	Individual	Thad Ness	American Electric Power (AEP)	X		X		X	X											

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

		Commenter	Organization	Industry Segment										
				1	2	3	4	5	6	7	8	9	10	
63.	Individual	Michael P Mertz	Southern California Edison Company	X		X		X	X					

- *Group 1 — IRC Standards Review Committee
- *Group 2 — Bonneville Power Administration
- *Group 3 — Northeast Power Coordinating Council
- *Group 4 — MRO NERC Standards Review Subcommittee

1. Please review the proposed incremental changes made to the version 1 VSLs to create a set of version 2 VSLs that is compatible with the version 2 CIP-002-2 through CIP-009-2 standards as posted for industry pre-ballot review commencing March 3, 2009. Then in the following table, please provide alternate language for any of the incremental changes to the VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

Summary Consideration: Based on stakeholder comments, the drafting team did make some changes to some of the sets of VSLs for CIP-002-2 (R4), CIP-003-2 (R 2.3 and R2.4), CIP-004-2 (R1 and R2.1), CIP-005-2 (R2,3), and CIP-006-2 (R1.1 and R1.4).

No changes were made to VSLs for CIP-007-2, CIP-008-2 or for CIP-009-2.

Most changes were either clarifying or format changes. In some cases, stakeholders identified additional descriptions of noncompliant performance that could be used to add more options to the already proposed VSLs – and where the proposed VSLs met the definitions for the proposed VSL category, the proposed VSLs were adopted.

All Changes Proposed by Stakeholders for VSLs for CIP-002-2 Cyber Security - Critical Cyber Asset Identification					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
BPA	R4			The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two or more of the following: 1) The risk-based assessment methodology for the identification of Critical Assets, 2) the list of Critical Assets and 3) the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, or 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
Response: Thank you for your comment, your suggested changes are being accepted.					

All Changes Proposed by Stakeholders for VSLs for CIP-003-2 Cyber Security – Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
BPA	R2.3			Changes to the delegated authority are not documented within thirty calendar days of the effective date.	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager.
<p>Response: Thank you for your comments. The drafting team has considered your suggested change to have additional levels of severity and has revised the VSLs for this requirement.</p>					
BPA	R2.4				Exceptions from the requirements of the cyber security policy were not authorized by the senior manager or delegate(s) and documented as required.
<p>Response: Thank you for your comment. Since the language of the requirement did not change between version one and version 2, the drafting team elected to maintain the version 1 VSL language for consistency for version 1 VSLs.</p>					

All Changes Proposed by Stakeholders for VSLs for CIP-004-2 Cyber Security – Personnel & Training					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
NPCC	R1	should use the same wording as the Standard as in “and implemented”	should use the same wording as the Standard as in “and implemented”	should use the same wording as the Standard as in “and implemented”	should use the same wording as the Standard as in “and implemented”
<p>Response: Thank you for your comment. The VSLs have been modified to reflect the language of the requirement.</p>					
BPA	R 2.1	At least one individual but less than 5% of personnel having unescorted access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having unescorted access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having unescorted access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having unescorted access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
<p>Response: Thank you for your comment. The language of the VSLs has been revised as suggested.</p>					

All Changes Proposed by Stakeholders for VSLs for CIP-005-2 Cyber Security – Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
BPA	R 2.3			The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
Response: Thank you for your comment. The language of the VSL has been revised to include your suggestion.					

All Changes Proposed by Stakeholders for VSLs for CIP-006-2 Cyber Security – Physical Security of Physical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
BPA	R 1.1		Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to Cyber Assets within the Electronic Security Perimeter.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and

All Changes Proposed by Stakeholders for VSLs for CIP-006-2 Cyber Security – Physical Security of Physical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
					documented alternative measures to control physical access to Cyber Assets within the Electronic Security Perimeter .
Response: Thank you for your comment. The language of the VSL has been revised to include your suggestion.					
BPA	R1.4				The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
Response: Thank you for your comment. The language of the VSL has been revised to include your suggestion.					
NPCC	R1.7	should use the same wording as the Standard	should use the same wording as the Standard	should use the same wording as the Standard	should use the same wording as the Standard
Response: Thank you for your comment. The drafting team believes the posted language is sufficient.					
Exelon	R2				Remove the sentence that appears prior to the OR statement as it is not necessary since it is covered by the other VSLs in this requirement. Sentence to eliminate is as follows: A Cyber Asset that

All Changes Proposed by Stakeholders for VSLs for CIP-006-2 Cyber Security – Physical Security of Physical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
					authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access.
Response: Thank you for your comments. The drafting team did not make any changes to the VSLs since the levels of VSLs are not duplicated.					
BPA	R7			The responsible entity did not retain physical access logs for at least ninety calendar days.	The Responsible Entity did not retain electronic access logs related to reportable incidents in accordance with the requirements of Standard CIP-008-2.
Response: Thank you for your comments. Since the technical language did not change, the drafting team has revised the VSLs to be consistent with version 1.					

2. Do you agree with the VRFs proposed for the version 2 CIP standards? If not, please identify which VRFs you disagree with and identify why.

Summary Consideration: All commenters except for one indicated agreement with the VRFs that were proposed, therefore the drafting team did not make any changes to the VRFs.

Organization	Yes or No	Question 3 Comment
Tampa Electric	Disagree	Time did not permit review, therefore we cannot agree at this time.
Exelon	Agree	
IESO	Agree	
BPA	Agree	
NPCC	Agree	
MRO NERC Standards Review Subcommittee	Agree	
Kansas City Power & Light	Agree	
IRC Standards Review Committee	Agree	
Southern California Edison Company	Agree	

3. If there any other comments you wish to provide (relative to the VSLs for CIP-002-2 through CIP-009-2) to the standard drafting team for Project 2008-06 Cyber Security Order 706 (version 2 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Summary Consideration: Based on stakeholder comments, the drafting team did make some changes to some of the sets of VSLs for CIP-002-2 (R4), CIP-003-2 (R 2.3 and R2.4), CIP-004-2 (R1 and R2.1), CIP-005-2 (R2,3), and CIP-006-2 (R1.1 and R1.4).

No changes were made to VSLs for CIP-007-2, CIP-008-2 or for CIP-009-2.

Most changes were either clarifying or format changes. In some cases, stakeholders identified additional descriptions of noncompliant performance that could be used to add more options to the already proposed VSLs – and where the proposed VSLs met the definitions for the proposed VSL category, the proposed VSLs were adopted.

Some commenters proposed modifications to requirements, and this is outside the scope of this VSL and VRF effort. Additional modifications to the requirements will be addressed in the next phase of modifications to the set of CIP standards.

Organization	Question 6 Comment
IESO	<p>Table 2, attached provides a summary assessment of the VRFs and VSLs for the Version 2 CIP standards. Examples cited in the comments below can be found in table 2.</p> <p>Similar problems as identified for the Version 1 CIP standards VSLs are also identified among the VSLs for the Version 2 CIP standards. An added inconsistency is the removal of some of the VSLs for the subrequirements after they are rolled-up to the main requirement. Examples re R2, R6 and R8 in CIP-006-2.</p> <p>Some subrequirements have become bullets. The main requirements' VSLs are dependent on which of the bulleted items are not complied with. It suggests that the bulleted items should in fact be subrequirements (conditions to meet the main requirement). We speculate that the SDT's intent is to roll-up non-compliance of subrequirements to the main requirement's VSLs, the approach is proper but this does not need a change from subrequirements to bullets. The latter is appropriate when the items are not required to be met, but rather they are listed as options or examples.</p>
<p>Response: Thank you for your comment.</p> <p>1. The roll up approach is used where appropriate to address industry concerns including the concern of double jeopardy. (Double jeopardy is assigning a penalty for violating a sub-requirement to both the sub-requirement and the primary requirement.)</p>	

Organization	Question 6 Comment
BPA	<p data-bbox="71 237 1108 261">2. Further concern on this topic should be raised through the standards drafting process.</p> <p data-bbox="422 302 527 326">General:</p> <p data-bbox="422 350 1927 407">Several of the VSLs for the version 2 standards include “(implemented)” after “established.” It is unclear why the parentheses are necessary and why the VSL does not just state “established and implemented.”</p> <p data-bbox="422 423 590 448">CIP-002-2, R4</p> <p data-bbox="422 472 2028 529">1. There doesn't seem to be any substantive difference between High and Severe. In fact High indicates that you don't have any of the 3. Severe indicates that they don't have 2 or more, which could actually be less severe than the High. They seem to be reversed.</p> <p data-bbox="422 553 2003 610">Our first suggestion therefore is that the definitions be switched so that the more egregious violation is listed under Severe and the less egregious is placed in the High.</p> <p data-bbox="422 626 2028 805">2. The proposed language change is cumbersome and could lead to a misinterpretation that a risk based methodology is used to identify Critical Cyber Assets. This would be incorrect. The basis for selection of Critical Cyber Assets is their presence within a Critical Asset, whether they are essential to the reliable operation of the Critical Asset and whether they meet the requirements of R3.1, or R3.2, or R3.3. There is no assessment involved that is a pure yes or no process. The risk-based methodology applies to the Critical Assets. We also recommend numbering each of the required elements to make it even clearer. The suggested replacements below are a bit longer, but make it clearer what the VSL statement is saying.</p> <p data-bbox="422 821 1335 846">Note: The definitions are also reversed to put them into the proper categories.</p> <p data-bbox="422 870 2028 959">Suggested Change High: The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two or more of the following: 1) The risk-based assessment methodology for the identification of Critical Assets, 2) the list of Critical Assets and 3) the list of Critical Cyber Assets (even if such lists are null.)</p> <p data-bbox="422 976 2028 1065">Suggested Change Severe: The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, or 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)</p> <p data-bbox="422 1081 621 1105">CIP-003-2, R 2.3</p> <p data-bbox="422 1114 1482 1138">Suggest breaking it out into two VSLs – rather than having it all under “severe” (see table).</p> <p data-bbox="422 1170 621 1195">CIP-004-2, R 2.1</p> <p data-bbox="422 1203 1524 1227">Suggest adding “unescorted” before “access” to align with wording in the standard (see table).</p> <p data-bbox="422 1260 621 1284">CIP-005-2, R 2.3</p> <p data-bbox="422 1292 1797 1317">Suggest breaking it out into two VSLs – rather than having it all under “severe”. Also change “or” to “and” (see table).</p>

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Organization	Question 6 Comment
	<p>CIP-006-2, R1.1 Reads poorly, suggested rewording and including “within the Electronic Security Perimeter” to each VSL (see table).</p> <p>CIP-006-2, R 1.4 Typo – R3 should be R4 to match version 2 standard (see table).</p> <p>CIP-006-2, R 7 Added a high VSL to correlate to retention of electronic access logs for 90 days, and for severe VSL added “related to reportable incidents” before log (see table).</p>
<p>Response: Thank you for your comments. The drafting team has addressed or responded to your specific concerns above in this consideration of comments document.</p>	
NPCC	<p>In CIP-004 the VSLs for R1 should use the same wording as the Standard. In CIP-006 the VSLs for R1.7 should use the same wording as the Standard.</p>
<p>Response: Thank you for your comments. The drafting team has addressed or responded to your specific concerns above in this consideration of comments.</p>	
NextEra Energy Resources, LLC	<p>General comment for both VSL’s and VRF’s for CIP-006-2, Use of the term “continuous” under R1.6 will need clarification.</p>
<p>Response: Thank you for your comments. Your concern is related to the language of the standard and should be addressed to the standards development process.</p>	
Tampa Electric	<p>We applaud the effort that has gone into this exercise. We know that it is not easy given the time constraints that NERC is facing. However, we feel the impact to the industry of these VSLs warrants that much more consideration be given to this project, and that time must be allowed to ensure that a quality product is delivered. We do not believe this document is at that point yet.</p> <p>NERC CIP drafting teams should give consideration to the number of items that they have out for review simultaneously at a time when the industry is working to meet the June and December 2009 compliance dates. We would have appreciated more time to review this, the TFE process, V2 of the standards, and all the new guidelines that were recently circulated.</p> <p>Additionally, we would like to know if the results and aggregated industry comments will be made available to the industry.</p>
<p>Response: Thank you for your comments. All comments and results associated with CIP Version 2 VSLs and VRFs are available to the industry on the NERC website.</p>	
IRC Standards Review Committee	<p>Table 2, attached provides a summary assessment of the VRFs and VSLs for the Version 2 CIP standards. Examples cited in the comments below can be found in table 2. Similar problems as identified for the Version 1 CIP standards VSLs are also identified among</p>

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Organization	Question 6 Comment
	the VSLs for the Version 2 CIP standards.
Response: Thank you for your comments. Table 2 provides “observations” but does not appear to provide recommendations for revisions to specific VSLs.	

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
CIP-002-2				
R1 R1.1 R1.2 R1.2.1 R1.2.2 R1.2.3 R1.2.4 R1.2.5 R1.2.6 R1.2.7	None	None	None	This standard remains virtually the same as in Version 1 except some cosmetic changes in R4.
R2	None	None	None	
R3 R3.1 R3.2 R3.2	None	None	None	
R4	Cosmetic	None	Cosmetic	Conforming changes
CIP-003-2				

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R1	None			
R1.1	None			
R1.2	None			
R1.3	None			
R2	Cosmetic	None	Cosmetic	Conforming changes
R2.1	Cosmetic	None	Cosmetic	Conforming changes
R2.2	None			
R2.3	New	Lower	New	Binary VSL: Severe only.
Response: Thank you for your comments.				
R2.4	None	Lower	New	VRF Same as R2.3 in V1; Binary VSL: Severe only.
Response: Thank you for your comments.				
R3	None			
R3.1	None			
R3.2	Cosmetic	None	Cosmetic	Conforming changes
R3.3	None			

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R4	None			
R4.1	None			
R4.2	None			
R4.3	None			
R5	None			
R5.1	None			
R5.2	None			
R5.3	None			
R6	None			
CIP-004-2				
R1	Cosmetic	None	Cosmetic	Conforming changes
R2	Minor wording	None	Minor	Conforming changes
R2.1	Minor wording	None	Minor	Conforming changes
R2.2 R2.2.1-R2.2.4	None			
R2.3	None			

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R3	Minor wording	None	Minor	Conforming changes
R3.1	None			
R3.2	None			
R3.3	None			
R4	None			
R4.1	None			
R4.2	None			
CIP-005-2				
R1	None			
R1.1	None			
R1.2	None			
R1.3	None			
R1.4	None			
R1.5	Cosmetic	None	Cosmetic	Conforming changes
R1.6	None			

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R2	None			
R2.1	None			
R2.2	None			
R2.3	Cosmetic	None	Cosmetic	Conforming changes
R2.4	None			
R2.5	None			
R2.6	None			
R3	None			
R3.1	None			
R3.2	None			
R4	None			
R4.1	None			
R4.2	None			
R4.3	None			
R4.4	None			

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R4.5	None			
R5	Cosmetic		None	
R5.1	Cosmetic		None	
R5.2	None			
R5.3	Cosmetic		None	
CIP-006-2				
R1	Minor wording	None	Minor	Conforming changes
R1.1	Minor wording	None	Minor	Conforming changes
R1.2	Cosmetic	None	Minor	Conforming changes
R1.3	None			
R1.4	Cosmetic	None	Minor	Conforming changes
R1.5	Cosmetic	None	Minor	Conforming changes
R1.6	Reworded	None	Minor	Conforming changes
R1.7	Minor wording	None	Minor	Conforming changes
R1.8	New	Lower	New	VRF same as R1.9 in V1; Binary VSL: Severe only.

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Additional Comments Submitted by the IRC Standards Review Committee and IESO

Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards

Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
Response: Thank you for your comments.				
R2	New	Medium	New	VSL has 4 levels whose assignments are dependent on meeting requirements in other CIP standards. This can be an issue.
Response: Thank you for your comments.				
R2.1	New	Medium	Removed	Rolled up to R2; but it has a VRF which by the general rule has to have a VSL!
Response: Thank you for your comments. The roll up approach is used where appropriate to address industry concerns including the concern of double jeopardy. (Double jeopardy is assigning a penalty for violating a sub-requirement to both the sub-requirement and the primary requirement.)				
R2.2	New	Medium	Removed	Rolled up to R2; but it has a VRF which by FERC's rule has to have a VSL!
Response: Thank you for your comments. The roll up approach is used where appropriate to address industry concerns including the concern of double jeopardy. (Double jeopardy is assigning a penalty for violating a sub-requirement to both the sub-requirement and the primary requirement.)				
R3	New	Medium	New	VRF is new; Binary VSL: Severe only.
Response: Thank you for your comments.				
R4	None (formerly R2)	Medium	Changed from VSLs for former R2).	VRF similar to R2 in V1; 3 VSLs from Moderate to Severe depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
Response: Thank you for your comments. Further concern on this topic should be raised through the standards drafting process.				

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R4.1–R4.4	Become bullets			See above comment.
Response: See response above.				
R5	None (formerly R3)	Medium	Changed from VSLs for former R3)	VRF similar to R3 in V1; 3 VSLs from Moderate to Severe depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
Response: Thank you for your comments Further concern on this topic should be raised through the standards drafting process.				
R5.1-R5.2	Become bullets			
R6	None (Formerly R4)	Lower	Changed from VSLs for former R4)	VRF similar to R4 in V1; 4 VSLs depending on which bulleted items the entity fails to implement. This suggests that the bulleted items should have remained as subrequirements.
Response: Thank you for your comments. Further concern on this topic should be raised through the standards drafting process.				
R6.1-R6.3	Become bullets			
R7	None (Formerly R5)	Lower	Similar to VSLs for former R5)	VRF similar to R5 in V1; Binary VSL: Severe only.
Response: Thank you for your comment.				
R8	Cosmetic (Formerly R6)	Medium	Similar to VSLs for former R6)	VRF similar to R6 in V1; 4 VSLs depending on which subrequirements the entity fails to comply.

Consideration of Comments for Project 2008-06 — Cyber Security Order 706 (CIP Version 2 VSLs and VRFs)

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
Response: Thank you for your comment.				
R8.1	None	Medium	Removed	VRF similar to R6.1 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC's rule has to have a VSL!
Response: Thank you for your comments. The roll up approach is used where appropriate to address industry concerns including the concern of double jeopardy. (Double jeopardy is assigning a penalty for violating a sub-requirement to both the sub-requirement and the primary requirement.)				
R8.2	Cosmetic	Lower	Removed	VRF similar to R6.2 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC's rule has to have a VSL!
Response: Thank you for your comments. The roll up approach is used where appropriate to address industry concerns including the concern of double jeopardy. (Double jeopardy is assigning a penalty for violating a sub-requirement to both the sub-requirement and the primary requirement.)				
R8.3	None	Lower	Removed	VRF similar to R6.3 in V1; Rolled up to R8 so there are no VSLs assigned; but it has a VRF which by FERC's rule has to have a VSL!
Response: Thank you for your comments. The roll up approach is used where appropriate to address industry concerns including the concern of double jeopardy. (Double jeopardy is assigning a penalty for violating a sub-requirement to both the sub-requirement and the primary requirement.)				
CIP-007-2				
R1	Cosmetic	None	None	None
R1.1	None			

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R1.2	None			
R1.3	None			
R2	Cosmetic	None	Minor	Conforming changes
R2.1	None	None	None	None
R2.2	None	None	None	None
R2.3	Minor wording	None	None	None
R3	Cosmetic	None	Minor	Conforming changes
R3.1	None	None	None	None
R3.2	Minor wording	None	None	None
R4	None			
R4.1	Minor wording	None	Minor	Conforming changes
R4.2	None			
R5	None			
R5.1	None			
R5.1.1	None			

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R5.1.2	None			
R5.1.3	Cosmetic	None	Minor	Conforming changes
R5.2	None			
R5.2.1	None			
R5.2.2	None			
R5.2.3	None			
R5.3	None			
R5.3.1	None			
R5.3.2	None			
R5.3.3	None			
R6	None			
R6.1	None			
R6.2	None			
R6.3	None			
R6.4	None			

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R6.5	None			
R7	Cosmetic	None	Minor	Conforming changes
R7.1	None			
R7.2	None			
R7.3	None			
R8	None			
R8.1	None			
R8.2	None			
R8.3	None			
R8.4	None			
R9	Cosmetic	None	Minor	Conforming changes
CIP-008-2				
R1	Wording changes	None	Minor	Conforming changes
R1.1	None			
R1.2	Minor wording			

Additional Comments Submitted by the IRC Standards Review Committee and IESO				
Table 2 — Summary of Comments on VSLs for Version 1 CIP Standards				
Standard and Requirement	Changes in Requirement	Changes in VRFs	Changes in VSLs	Assessment
R1.3	None			
R1.4	Cosmetic			
R1.5	None			
R1.6	Major changes			
R2	None			
CIP-009-2				
R1	None			
R1.1	None			
R1.2	None			
R2	None			
R3	Cosmetic	None	Minor	Conforming changes
R4	None			
R5	None			

Standards Announcement

Ballot Pool and Pre-ballot Window

August 11–September 10, 2009

Now available at: <https://standards.nerc.net/BallotPool.aspx>

Project 2008-06: Cyber Security (VRFs and VSLs for Version 2 CIP Standards)

Proposed Violation Severity Levels (VSLs) for Critical Infrastructure Protection (CIP) standards CIP-002-2 through CIP-009-2 and Violation Risk Factors (VRFs) for CIP-003-2 and CIP-006-2 are posted for a 30-day pre-ballot review. Registered Ballot Body members may join the ballot pool to be eligible to vote on these items **until 8 a.m. EDT on September 10, 2009**.

During the pre-ballot window, members of the ballot pool may communicate with one another by using their “ballot pool list server.” (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list server for this ballot pool is: [bp-2008-06_CIP_VSL_VRF_in](#).

Next Steps

Voting will begin shortly after the pre-ballot review closes.

Project Background

Standards CIP-002-2 through CIP-009-2 have been approved by stakeholders; the purpose of this part of the project is to complete the VSLs (for CIP-002-2 through CIP-009-2) and VRFs (for CIP-003-2 and CIP-006-2) for those standards. This step is part of the overall Project 2008-06 — Cyber Security Order 706.

VSLs: The posted VSLs are those associated with requirements that were modified when converting standards CIP-002-1 through CIP-009-1 into CIP-002-2 through CIP-009-2.

VRFs: The posted VRFs are for the two standards with VRF changes resulting from modifications made during the transition from standards CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2:

- CIP-003-2 Security Management Controls
- CIP-006-2 Physical Security of Critical Cyber Assets.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Standards Development Process

The [Reliability Standards Development Procedure](#) contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

*For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*

Note — This report shows only those VSLs that are associated with requirements that were modified when converting CIP-002-1 through CIP-009-1 into CIP-002-2 through CIP-009-2. Stakeholders have already balloted and approved the VSLs that are associated with requirements that were not changed.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards (Project 2008-06):

Index:

Standard Number CIP-002-2 Critical Cyber Asset Identification2

Standard Number CIP-003-2 Security Management Controls3

Standard Number CIP-004-2 Personnel & Training.....5

Standard Number CIP-005-2 Electronic Security Perimeter(s).....7

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets8

Standard Number CIP-007-2 Systems Security Management.....16

Standard Number CIP-008-2 Incident Reporting and Response Planning.....19

Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets20

Standard Number CIP-002-2 — Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1.	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.3.	N/A	N/A	<p>The identification of a senior manager’s delegate does not include at least one of the following; name, title, or date of the designation,</p> <p>OR</p> <p>The document is not approved by the senior manager,</p> <p>OR</p> <p>Changes to the delegated authority are not documented within thirty calendar days of the effective date.</p>	A senior manager’s delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; or changes to the delegated authority are not documented within thirty calendar days of the effective date.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.4.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3.2.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
R2.	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, implement, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1.	At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
R3.	N/A	The Responsible Entity has a personnel risk assessment	The Responsible Entity has a personnel risk assessment program	The Responsible Entity does not have a documented personnel risk

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.</p>	<p>as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.</p>	<p>assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access.</p> <p>OR</p> <p>The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.</p>

Standard Number CIP-005-2 — Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3, Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.
R2.3.	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created and implemented but did not maintain a physical security plan.</p>	<p>The Responsible Entity did not document, implement, and maintain a physical security plan.</p>
R1.1.	N/A	<p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.</p>	<p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.</p>	<p>The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.</p> <p>OR</p> <p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to the Critical such Cyber Assets within the Electronic Security Perimeter.</p>

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.2.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not-address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
R1.6.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7.	N/A	N/A	The Responsible Entity's physical security plan addresses a process for updating the physical security plan within-thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or reconfiguration.
R1.8.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R1.9.	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
R3.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4.	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
R5.	N/A	<p>The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following</p>	<p>The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following</p>	<p>The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:</p>

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-2.
R6.	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. 	<p>method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. 	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. 	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
R7.	The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained physical access logs for less than 45 calendar days.
R8.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2,	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	and R8.3.	R8.3.	R8.3.	

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement) , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1.	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.</p>
R5.1.3.	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.</p>
R7.	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not maintain</p>	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address redeployment as specified in R7.2.</p>	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1.</p>	<p>The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.</p>

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	records as specified in R7.3.			
R9.	N/A	N/A	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.</p>

Standard Number CIP-008-2 — Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

Standard Number CIP-009-2 — Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 30 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

Note — this document only shows those VSLs that were changed as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2.

This redline is showing the changes made between the balloted set of Version 1 VSLs and the proposed Version 2 VSLs.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards (Project 2008-06):

Index:

Standard Number CIP-002-2 Critical Cyber Asset Identification2
Standard Number CIP-003-2 Security Management Controls3
Standard Number CIP-004-2 Personnel & Training.....6
Standard Number CIP-005-2 Electronic Security Perimeter(s).....10
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....12
Standard Number CIP-007-2 Systems Security Management.....26
Standard Number CIP-008-2 Incident Reporting and Response Planning.....31
Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets32

Standard Number CIP-002-2 — Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4. (Version 1)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
R4 (Proposed changes to align with version 2)	N/A	<u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)</u>	<u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)</u>	<u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)</u>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	N/A	N/A	The Responsible Entity has not assigned a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1. (Version 1)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.3. (Version 1)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exception from the requirements of the cyber security policy as required.

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.3 (Proposed changes to align with version 2)	N/A N/A		<p><u>The identification of a senior manager’s delegate does not include at least one of the following: name, title, or date of the designation.</u></p> <p><u>OR</u></p> <p><u>The document is not approved by the senior manager.</u></p> <p><u>OR</u></p> <p><u>Changes to the delegated authority are not documented within thirty calendar days of the effective date.</u></p>	A senior manager’s delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; or changes to the delegated authority are not documented within thirty calendar days of the effective date.
New R2.4 (Proposed to align with version 2)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document as required , <u>any</u> exceptions from the requirements of the cyber security policy <u>as required</u> .
R3.2. (Version 1)	N/A	N/A	<p>The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either:</p> <p>1) an explanation as to why the exception is necessary, or</p>	<p>The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both:</p> <p>1) an explanation as to why the exception is necessary, and</p>

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
			2) any compensating measures or a statement accepting risk.	2) any compensating measures or a statement accepting risk.
R3.2 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
R1 (Proposed changes to align with version 2)	The Responsible Entity established, (implemented) , and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, (implement) , nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, (implement) , maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
R2. (Version 1)	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Proposed changes to align with version 2)	The Responsible Entity established _(implemented)_ and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish _(implement)_ nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish _(implement)_ , maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1. (Version 1)	At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.
R2.1 (Proposed changes to align with version 2)	At least one individual but less than 5% of personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3. (Version 1)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in sixty (60) days or more of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.
R3 (Proposed changes to align with version 2)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after in sixty (60) days or more of such personnel were being granted such access except in specified circumstances such as an emergency.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 — Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5. (Version 1)	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
R1.5 (Proposed changes to align with version 2)	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3, Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.
R2.3. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not maintain a procedure for securing dial-up access to the Electronic

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 — Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Security Perimeter(s) where applicable.
R2.3 (Proposed changes to align with version 2)	N/A N/A		<u>The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.</u>	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created but did not maintain a physical security plan.</p>	The Responsible Entity did not create and maintain a physical security plan.
R1 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created and implemented but did not maintain a physical security plan.</p>	The Responsible Entity did not create and document, implement, and maintain a physical security plan.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.1. (Version 1)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical Cyber Assets.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical Cyber Assets.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical access to the Critical Cyber Assets.
R1.1 (Proposed changes to align with version 2)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical such Cyber Assets <u>within the Electronic Security Perimeter</u> .	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical such Cyber Assets <u>within the Electronic Security Perimeter</u> .	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not deployed and documented alternative measures to control physical to the Critical-such Cyber Assets within the Electronic Security Perimeter .
R1.2. (Version 1)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify all access points through each Physical Security Perimeter but not measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.2 (Proposed changes to align with version 2)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.4 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the appropriate use of physical access controls as described in Requirement R3.
R1.4 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the address the appropriate use of physical access controls as described in

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R4 .
R1.5 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan does not include either the procedures for reviewing access authorization requests or revocation of access authorization, in accordance with CIP-004 Requirement R4.	The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
R1.5 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan does not include address either the procedures process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004- 2 Requirement R4.	The Responsible Entity's physical security plan does not include address the process procedures for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004- 2 Requirement R4.
R1.6 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for escorted access within the physical security perimeter.
R1.6 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures-address the process for continuous escorted access within the physical security perimeter.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration but the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.
R1.7 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan includes addresses a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within 90 thirty calendar days of the completion of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include address a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.8 (Version 1)	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.
R1.8 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Proposed changes to align with version 2)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Version 1)	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.
R2 (Proposed changes to align with version 2)	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
New R2.1 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
New R2.2 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
R3 (Version 1)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirements R3.1 or R3.2.	Requirements R3.1 or R3.2.	OR One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.
R3 (Proposed changes to align with version 2)	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4 (Version 1)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4 (Proposed changes to align with version 2)	N/A	<p>The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5 (Version 1)	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs for at least ninety calendar days.
R5 (Proposed changes to align with version 2)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. <p>OR</p> <p>An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-</p>

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				008-2.
R6 (Version 1)	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include one of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include two of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include any of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.
R6 (Proposed changes to align with version 2)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record 	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by 	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of 	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
New R7 (Proposed changes to align with version 2)	<u>The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.</u>	<u>The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.</u>	<u>The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.</u>	<u>The Responsible Entity retained physical access logs for less than 45 calendar days.</u>
New R8 (Proposed changes to align with version 2)	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.
New R8.1 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
New R8.2 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)
New R8.3 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2 (Proposed changes to align with version 2)	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. (Version 1)	The Responsible Entity established and documented, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established but did not document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish nor document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3 (Proposed changes to	The Responsible Entity established (implemented) and documented, either separately or	The Responsible Entity established (implemented) but did not document , either	The Responsible Entity documented but did not establish (implement) , either	The Responsible Entity did not establish (implement) nor document , either separately or as

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
align with version 2)	as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R4.1. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.
R5.1.3. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
R5.1.3 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R7. (Version 1)	The Responsible Entity established formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not maintain records as specified in R7.3.	The Responsible Entity established formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address redeployment as specified in R7.2.	The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R7 (Proposed changes to align with version 2)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not maintain records as specified in R7.3.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.
R9 (Version 1)	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually or the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R9 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>or the The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty ninety calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty ninety calendar days of the change being completed.</p>

Standard Number CIP-008-2 — Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6	The Responsible Entity has not developed a Cyber Security Incident response plan.
R1 (Proposed changes to align with version 2)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

Standard Number CIP-009-2 — Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3 (Version 1)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.
R3 (Proposed changes to align with version 2)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery

Standard Number CIP-009-2 — Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	30 but less than or equal to 120 calendar days of the change.	than or equal to 150 calendar days of the change.	than or equal to 180 calendar days of the change.	plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

Note — this document only shows those VSLs that were changed as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2.

This redline is showing the initial changes made between Version 1 and Version 2 (shown in red text), as well as the additional changes made based on stakeholder comments (shown in blue text).

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards (Project 2008-06):

Index:

Standard Number CIP-002-2 Critical Cyber Asset Identification2

Standard Number CIP-003-2 Security Management Controls3

Standard Number CIP-004-2 Personnel & Training.....6

Standard Number CIP-005-2 Electronic Security Perimeter(s).....10

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....12

Standard Number CIP-007-2 Systems Security Management.....26

Standard Number CIP-008-2 Incident Reporting and Response Planning.....31

Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets32

Standard Number CIP-002-2 — Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4. (Version 1)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
R4 (Proposed changes to align with version 2)	N/A	N/A <u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)</u>	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.) <u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)</u>	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both two or more of the following: the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) <u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)</u>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	N/A	N/A	The Responsible Entity has not assigned a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1. (Version 1)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.3. (Version 1)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exception from the requirements of the cyber security policy as required.

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.3 (Proposed changes to align with version 2)	N/A N/A		<p>N/A</p> <p><u>The identification of a senior manager’s delegate does not include at least one of the following: name, title, or date of the designation.</u></p> <p><u>OR</u></p> <p><u>The document is not approved by the senior manager.</u></p> <p><u>OR</u></p> <p><u>Changes to the delegated authority are not documented within thirty calendar days of the effective date.</u></p>	A senior manager’s delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; or changes to the delegated authority are not documented within thirty calendar days of the effective date.
New R2.4 (Proposed to align with version 2)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document as required , <u>any</u> exceptions from the requirements of the cyber security policy <u>as required</u> .

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.2. (Version 1)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.
R3.2 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
R1 (Proposed changes to align with version 2)	The Responsible Entity established, (implemented) , and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, (implement) , nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, (implement) , maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
R2. (Version 1)	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Proposed changes to align with version 2)	The Responsible Entity established _(implemented)_ and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish _(implement)_ nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish _(implement)_ , maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1. (Version 1)	At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.
R2.1 (Proposed changes to align with version 2)	At least one individual but less than 5% of personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	15% or more of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3. (Version 1)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in sixty (60) days or more of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.
R3 (Proposed changes to align with version 2)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after in sixty (60) days or more of such personnel were being granted such access except in specified circumstances such as an emergency .	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 — Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5. (Version 1)	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
R1.5 (Proposed changes to align with version 2)	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3, Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.
R2.3. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not maintain a procedure for securing dial-up access to the Electronic

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 — Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Security Perimeter(s) where applicable.
R2.3 (Proposed changes to align with version 2)	N/A	N/A	N/A The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created but did not maintain a physical security plan.</p>	The Responsible Entity did not create and maintain a physical security plan.
R1 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created and implemented but did not maintain a physical security plan.</p>	The Responsible Entity did not create and document, implement, and maintain a physical security plan.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.1. (Version 1)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical Cyber Assets.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical Cyber Assets.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical access to the Critical Cyber Assets.
R1.1 (Proposed changes to align with version 2)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical such Cyber Assets <u>within the Electronic Security Perimeter</u> .	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical such Cyber Assets <u>within the Electronic Security Perimeter</u> .	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not deployed and documented alternative measures to control physical to the Critical-such Cyber Assets within the Electronic Security Perimeter .
R1.2. (Version 1)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify all access points through each Physical Security Perimeter but not measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.2 (Proposed changes to align with version 2)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.4 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the appropriate use of physical access controls as described in Requirement R3.
R1.4 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the address the appropriate use of physical access controls as described in

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R3 R4.
R1.5 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan does not include either the procedures for reviewing access authorization requests or revocation of access authorization, in accordance with CIP-004 Requirement R4.	The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
R1.5 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan does not include address either the procedures process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004- 2 Requirement R4.	The Responsible Entity's physical security plan does not include address the process procedures process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004- 2 Requirement R4.
R1.6 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for escorted access within the physical security perimeter.
R1.6 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures address the process process for continuous escorted access within the physical security perimeter.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration but the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.
R1.7 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan includes addresses a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within 90 thirty calendar days of the completion of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include address a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.8 (Version 1)	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.
R1.8 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Proposed changes to align with version 2)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Version 1)	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.
R2 (Proposed changes to align with version 2)	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
New R2.1 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
New R2.2 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
R3 (Version 1)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirements R3.1 or R3.2.	Requirements R3.1 or R3.2.	OR One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.
R3 (Proposed changes to align with version 2)	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4 (Version 1)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4 (Proposed changes to align with version 2)	N/A	<p>The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5 (Version 1)	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs for at least ninety calendar days.
R5 (Proposed changes to align with version 2)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. <p>OR</p> <p>An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-</p>

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				008-2.
R6 (Version 1)	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include one of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include two of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include any of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.
R6 (Proposed changes to align with version 2)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record 	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by 	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of 	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
<p>New R7 (Proposed changes to align with version 2)</p>	<p>of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.</p> <p><u>The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.</u> N/A</p>	<p>security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.</p> <p><u>The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.</u> N/A</p>	<p>physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.</p> <p><u>The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.</u> N/A</p>	<p>physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.</p> <p><u>The Responsible Entity retained physical access logs for less than 45 calendar days.</u> The Responsible Entity did not retain electronic access logs in accordance with the requirements of Standard CIP-008-2.</p>
<p>New R8 (Proposed changes to align with version 2)</p>	<p>The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.</p>	<p>The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.</p>	<p>The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.</p>	<p>The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.</p>
<p>New R8.1 (Proposed changes to align with</p>	<p>N/A (Rolled up into R8.)</p>	<p>N/A (Rolled up into R8.)</p>	<p>N/A (Rolled up into R8.)</p>	<p>N/A (Rolled up into R8.)</p>

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
version 2)				
New R8.2 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)
New R8.3 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2 (Proposed changes to align with version 2)	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. (Version 1)	The Responsible Entity established and documented, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established but did not document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish nor document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3 (Proposed changes to	The Responsible Entity established (implemented) and documented, either separately or	The Responsible Entity established (implemented) but did not document , either	The Responsible Entity documented but did not establish (implement) , either	The Responsible Entity did not establish (implement) nor document , either separately or as

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
align with version 2)	as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R4.1. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.
R5.1.3. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
R5.1.3 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R7. (Version 1)	The Responsible Entity established formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not maintain records as specified in R7.3.	The Responsible Entity established formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address redeployment as specified in R7.2.	The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R7 (Proposed changes to align with version 2)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not maintain records as specified in R7.3.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.
R9 (Version 1)	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually or the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R9 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>or the The Responsible Entity did not document Cchanges resulting from modifications to the systems or controls within thirty ninety calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were Cchanges resulting from modifications to the systems or controls documented within thirty ninety calendar days of the change being completed.</p>

Standard Number CIP-008-2 — Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6	The Responsible Entity has not developed a Cyber Security Incident response plan.
R1 (Proposed changes to align with version 2)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

Standard Number CIP-009-2 — Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3 (Version 1)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.
R3 (Proposed changes to align with version 2)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery

Standard Number CIP-009-2 — Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	30 but less than or equal to 120 calendar days of the change.	than or equal to 150 calendar days of the change.	than or equal to 180 calendar days of the change.	plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2. Only the 15 VRFs shown in red text are “new.” There were no changes to these VRFs based on stakeholder comments.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 2 CIP-002-2 thru CIP-009-2 Standards:

Index:

Standard Number CIP-003-2 Security Management Controls2
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....3

Standard Number CIP-003 — Security Management Controls			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.	LOWER
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2 R2.3.		Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2 R2.4.		The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8.	Annual review of the physical security plan.	LOWER
CIP-006-2	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM
CIP-006-2	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-2	R4.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets 	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been 	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		<p>opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.</p> <ul style="list-style-type: none"> Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	
CIP-006-2	R6.	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4 	LOWER
CIP-006-2	R7.	<p>Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.</p>	LOWER
CIP-006-2	R8.	<p>Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:</p>	MEDIUM
CIP-006-2	R8.1.	<p>Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.</p>	MEDIUM
CIP-006-2	R8.2.	<p>Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.</p>	LOWER
CIP-006-2	R8.3.	<p>Retention of outage records regarding access controls, logging, and monitoring for a</p>	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		minimum of one calendar year.	

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2. Only the 15 VRFs shown in red text are “new.” There were no changes to these VRFs based on stakeholder comments.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 2 CIP-002-2 thru CIP-009-2 Standards:

Index:

Standard Number CIP-003-2 Security Management Controls2
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....3

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-003 — Security Management Controls			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.	LOWER
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2	R2.3. (New)	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2	R2.4. (New – similar to version 1 R2.3 which was LOWER)	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8. (New – similar to version 1 R1.9 which was LOWER)	Annual review of the physical security plan.	LOWER
CIP-006-2	R2. (New)	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers,	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		shall:	
CIP-006-2	R2.1. (New)	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2. (New)	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM
CIP-006-2	R3. (New)	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-2	R4. (New – Similar to version 1 R2, R2.1, R2.2, R2.3, and R2.4 combined – which were all MEDIUM)	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets 	MEDIUM
CIP-006-2	R5. (New – Similar to version 1 R3, R3.1, and R3.2 combined – R3)	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring	MEDIUM

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
	and R3.1 were MEDIUM and R3.2 was LOWER)	<p>methods shall be used:</p> <ul style="list-style-type: none"> Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	
CIP-006-2	R6. (New – Similar to version 1 R4, R4.1, R4.2, and R4.3 combined – which were all LOWER)	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4 	LOWER
CIP-006-2	R7. New – Similar to version 1 R5 – which was LOWER)	<p>Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.</p>	LOWER
CIP-006-2	R8. (New – Similar to version 1 R6 – which was MEDIUM)	<p>Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:</p>	MEDIUM
CIP-006-2	R8.1.	<p>Testing and maintenance of all physical security mechanisms on a cycle no longer than</p>	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
	(New – Similar to version 1 R6.1 – which was MEDIUM)	three years.	
CIP-006-2	R8.2. (New – Similar to version 1 R6.2 – which was LOWER)	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-2	R8.3. (New – Similar to version 1 R6.3 – which was LOWER)	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER

Standards Announcement Initial Ballot Window Open September 10–21, 2009

Now available at: <https://standards.nerc.net/CurrentBallots.aspx>

Project 2008-06: Cyber Security (VRFs and VSLs for Version 2 CIP Standards)

An initial ballot window for proposed Violation Severity Levels (VSLs) for Critical Infrastructure Protection (CIP) standards CIP-002-2 through CIP-009-2 and Violation Risk Factors (VRFs) for CIP-003-2 and CIP-006-2 is now open **until 8 p.m. EDT on September 21, 2009**.

Instructions

Members of the ballot pool associated with this project may log in and submit their votes from the following page: <https://standards.nerc.net/CurrentBallots.aspx>

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

Standards CIP-002-2 through CIP-009-2 have been approved by stakeholders; the purpose of this part of the project is to complete the VSLs (for CIP-002-2 through CIP-009-2) and VRFs (for CIP-003-2 and CIP-006-2) for those standards. This step is part of the overall Project 2008-06 — Cyber Security Order 706.

VSLs: The posted VSLs are those associated with requirements that were modified when converting standards CIP-002-1 through CIP-009-1 into CIP-002-2 through CIP-009-2.

VRFs: The posted VRFs are for the two standards with VRF changes resulting from modifications made during the transition from standards CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2:

- CIP-003-2 Security Management Controls
- CIP-006-2 Physical Security of Critical Cyber Assets.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Standards Development Process

The [Reliability Standards Development Procedure](#) contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

*For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*

Standards Announcement Initial Ballot Results

Now available at: <https://standards.nerc.net/Ballots.aspx>

Project 2008-06: Cyber Security (VRFs and VSLs for Version 2 CIP Standards)

The initial ballot for proposed Violation Severity Levels (VSLs) for critical infrastructure protection (CIP) standards CIP-002-2 through CIP-009-2 and Violation Risk Factors (VRFs) for CIP-003-2 and CIP-006-2 ended on September 21, 2009.

Ballot Results

Voting statistics are listed below, and the [Ballot Results](#) Web page provides a link to the detailed results:

Quorum: 87.45%
Approval: 94.18%

Since at least one negative ballot included a comment, these results are not final. A second (or recirculation) ballot must be conducted. Ballot criteria are listed at the end of the announcement.

Next Steps

As part of the recirculation ballot process, the drafting team must draft and post responses to voter comments. The drafting team will also determine whether or not to make revisions to the balloted item(s). Should the team decide to make revisions, the revised item(s) will return to the initial ballot phase.

Project Background

Standards CIP-002-2 through CIP-009-2 have been approved by stakeholders; the purpose of this part of the project is to complete the VSLs and VRFs for those standards. This step is part of the overall Project 2008-06 — Cyber Security Order 706.

The posted VSLs are those associated with requirements that were modified when converting standards CIP-002-1 through CIP-009-1 into CIP-002-2 through CIP-009-2. The posted VRFs are for the two standards with VRF changes resulting from modifications made during the transition from standards CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2:

- CIP-003-2 — Security Management Controls
- CIP-006-2 — Physical Security of Critical Cyber Assets.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Standards Development Process

The [Reliability Standards Development Procedure](#) contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Ballot Criteria

Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

*For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*

User Name

Password

Log in

Register

- Ballot Pools
- Current Ballots
- Ballot Results
- Registered Ballot Body
- Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Cyber Security (VRFs and VSLs for Version 2 CIP Standards)_in
Ballot Period:	9/10/2009 - 9/21/2009
Ballot Type:	Initial
Total # Votes:	209
Total Ballot Pool:	239
Quorum:	87.45 % The Quorum has been reached
Weighted Segment Vote:	94.18 %
Ballot Results:	The standard will proceed to recirculation ballot.

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain # Votes	No Vote
			# Votes	Fraction	# Votes	Fraction		
1 - Segment 1.	63	1	44	0.917	4	0.083	9	6
2 - Segment 2.	9	0.6	6	0.6	0	0	3	0
3 - Segment 3.	54	1	42	0.955	2	0.045	5	5
4 - Segment 4.	14	1	9	0.9	1	0.1	1	3
5 - Segment 5.	44	1	26	0.897	3	0.103	8	7
6 - Segment 6.	33	1	22	1	0	0	4	7
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	9	0.7	7	0.7	0	0	0	2
9 - Segment 9.	8	0.6	6	0.6	0	0	2	0
10 - Segment 10.	5	0.5	4	0.4	1	0.1	0	0
Totals	239	7.4	166	6.969	11	0.431	32	30

Individual Ballot Pool Results

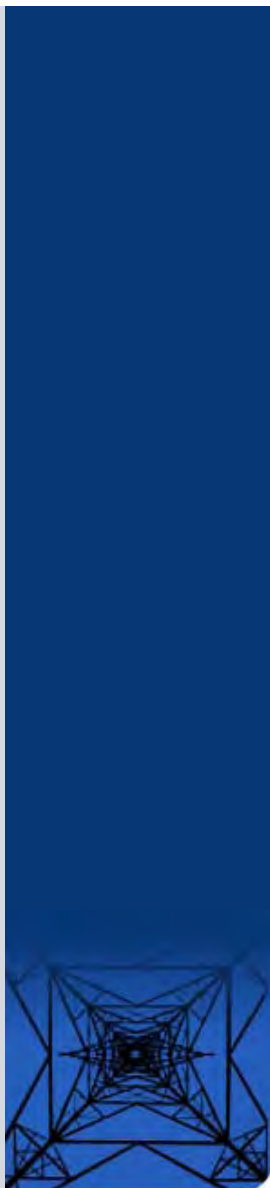
Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Abstain	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	

1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	City Utilities of Springfield, Missouri	Jeff Knottek		
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	E.ON U.S. LLC	Larry Monday		
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Albert Poire	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Kissimmee Utility Authority	Joe B Watson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	Rodney Hawkins	Negative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Abstain	
1	National Grid	Manuel Couto	Affirmative	
1	Nebraska Public Power District	Richard L. Koch		
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura		
1	Ohio Valley Electric Corp.	Robert Matthey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Oncor Electric Delivery	Charles W. Jenkins	Abstain	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Negative	
1	PP&L, Inc.	Ray Mammarella	Abstain	
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Abstain	
1	SaskPower	Wayne Guttormson	Abstain	
1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Abstain	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	View
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Affirmative	
1	Southwestern Power Administration	Gary W Cox	Affirmative	
1	Tampa Electric Co.	Thomas J. Szelistowski	Abstain	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L. Pieper	Affirmative	
2	Alberta Electric System Operator	Jason L. Murray	Abstain	
2	BC Transmission Corporation	Faramarz Amjadi	Affirmative	
2	California ISO	Greg Tillitson	Abstain	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Abstain	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Affirmative	

3	Allegheny Power	Bob Reeping	Affirmative	
3	American Electric Power	Raj Rana	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Power Agency	Duane S. Dahlquist	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Farmington	Linda R. Jacobson	Affirmative	
3	City of Lansing by its Board of Water and Light	David C Bolan		
3	City Public Service of San Antonio	Edwin Les Barrow	Affirmative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Abstain	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W Pourciau	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Affirmative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory David Woessner	Negative	
3	Lakeland Electric	Mace Hunter	Affirmative	
3	Lincoln Electric System	Bruce Merrill		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Abstain	
3	Manitoba Hydro	Greg C Parent	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscataine Power & Water	John Bos	Affirmative	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters		
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	Zack Dusenbury	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	View
3	Tampa Electric Co.	Ronald L. Donahey		
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt		
4	City of Troy Utilities	Brian M Chandler		
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Northern California Power Agency	Fred E. Young	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	

4	Seminole Electric Cooperative, Inc.	Steven R. Wallace		
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Abstain	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Consolidated Edison Co. of New York	Edwin E Thompson	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Robert Smith	Affirmative	
5	Edison Mission Energy	Ellen Oswald	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner		
5	FPL Energy	Benjamin Church		
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	JEA	Donald Gilbert	Abstain	
5	Kansas City Power & Light Co.	Scott Heidtbrink		
5	Lakeland Electric	Thomas J Trickey	Negative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Louisville Gas and Electric Co.	Charlie Martin	Abstain	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Abstain	
5	Orlando Utilities Commission	Richard Kinan	Negative	View
5	PacifiCorp Energy	David Godfrey	Abstain	
5	Portland General Electric Co.	Gary L Tingley		
5	PPL Generation LLC	Mark A. Heimbach	Abstain	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
5	RRI Energy	Thomas J. Bradish	Affirmative	
5	Sacramento Municipal Utility District	Bethany Wright	Affirmative	
5	Salt River Project	Glen Reeves	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Southeastern Power Administration	Douglas Spencer	Abstain	
5	Tampa Electric Co.	Frank L Busot	Abstain	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Chris Lyons	Abstain	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Eugene Water & Electric Board	Daniel Mark Bedbury		
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell		
6	Great River Energy	Donna Stephenson		
6	Kansas City Power & Light Co.	Thomas Saitta	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Louisville Gas and Electric Co.	Daryn Barker	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PacifiCorp	Gregory D Maxfield	Affirmative	

6	Portland General Electric Co.	John Jamieson	Affirmative	
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson	Affirmative	
6	Salt River Project	Mike Hummel	Affirmative	
6	Santee Cooper	Suzanne Ritter	Abstain	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Southern California Edison Co.	Marcus V Lotto	Affirmative	View
6	Tampa Electric Co.	Joann Wehle		
6	Western Area Power Administration - UGP Marketing	John Stonebarger		
6	Xcel Energy, Inc.	David F. Lemmons	Abstain	
8	Dennis Neitzel	Dennis Neitzel	Affirmative	
8	Edward C Stein	Edward C Stein	Affirmative	
8	Encari	Matthew E. Luallen		
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz	Affirmative	
8	Volkman Consulting, Inc.	Terry Volkman	Affirmative	
8	Wally Magda	Wally Magda	Affirmative	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	Maine Public Utilities Commission	Jacob A McDermott	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Service Commission of South Carolina	Philip Riley	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	View
10	ReliabilityFirst Corporation	Jacqui Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Negative	View
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	



Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
 Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

[Account Log-In/Register](#)

Copyright © 2008 by the North American Electric Reliability Corporation. : All rights reserved.
 A New Jersey Nonprofit Corporation

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Summary Consideration:

The drafting team corrected an error in the Cyber Security VSLs for CIP-003-2 R 2.3 based on balloter comments so that the Severe VSL describes performance that is more noncompliant than the performance for the High VSL. This was the only modification to the VSLs and VRFs for the Cyber Security Standards version 2.

One comment submitted suggests a wording change for a future version of CIP003 R2.4. This comment has been forwarded to the Standards Drafting Team working on Version 4 of the CIP standards.

Most comments submitted with a negative ballot indicated that the VSLs need to account for “risk” and the DT explained that the risk associated with noncompliance is identified by the Violation Risk Factor, not the Violation Severity Level. Violation Severity Levels identify degrees of noncompliant performance without regard to reliability-related risk. Some balloters proposed modifications to the requirements, and this is outside the scope of this project.

In proposing VSLs, the DT gave consideration to the guidelines provided by FERC in its June 19, 2008 Order on Violation Severity Levels:

From: ORDER ON VIOLATION SEVERITY LEVELS PROPOSED BY THE ELECTRIC RELIABILITY ORGANIZATION (Issued June 19, 2008)
17. For purposes of Commission review, and as a useful tool in the future development of new, or revision of current Violation Severity Levels, the Commission has developed four guidelines for evaluating the validity of Violation Severity Level assignments:

- (1) Violation Severity Level assignments should not have the unintended consequence of lowering the current level of compliance;
- (2) Violation Severity Level assignments should ensure uniformity and consistency among all approved Reliability Standards in the determination of penalties;
- (3) Violation Severity Level assignments should be consistent with the corresponding requirement; and
- (4) Violation Severity Level assignments should be based on a single violation, not on a cumulative number of violations. These guidelines will provide a consistent and objective means for assessing, *inter alia*, the consistency, fairness and potential consequences of Violation Severity Level assignments.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.¹

¹ The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
John D. Martinsen	Public Utility District No. 1 of Snohomish County	4	Negative	Although the District reviews the Critical Assets and the list of Critical Cyber Assets on an annual basis, we do not believe the lack of a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list should be considered a Severe VSL. Performing the review and assessment tasks that may uncover reliability exposures is significantly more important than a signature. We believe this is another case where the requirements and exposure to penalties focus on documentation and have little to no impact on regional reliability or reducing the risks of wide-spread cascading outages.
<p>Response: Thank you for your comment. As defined, a VSL is an after the fact look at how well the responsible entity met the intent of the requirement. This is quite different from a violation risk factor which determines (if the requirement were to be violated) what would be the impact to the reliability of the bulk electric system.</p> <p>In assigning VSLs it is assumed that the requirement has been violated and the question that remains is how severely the intent of the requirement has been missed. For example if the requirement states that X must be documented and the responsible entity has not documented X then the intent of the requirement has been missed and therefore the severity level must be severe. Similar conditions apply to any and all requirements that are binary in nature (i.e. the requirement is either met or not met) in that not meeting the requirement can only be a severe violation level. The impact on the BES would be taken care of by the violation risk factor. A documentation type of requirement would likely have a lower risk factor than a requirement for specific action (by the responsible entity) that impacts the BES.</p>				
Richard Kinas	Orlando Utilities Commission	5	Negative	CIP-006 R3 VSL is arbitrarily harsh at a Sever level for "A cyber Asset". Depending on how many assets are used to implement an Entities ESP control system, a miss of a single component that is potnetially composed of dozens of such assets does not seem to match the violation.
<p>Response: Thank you for your comment. Because CIP-006-2 R3 refers to cyber assets used in the access control and/or monitoring of access to the Electronic Security Perimeter. Failure to protect any such cyber asset is considered to be a severe violation due to the potential vulnerability created by such a lack of protection.</p> <p>In assigning VSLs it is assumed that the requirement has been violated and the question that remains is how severely the intent of the requirement has been missed. For example if the requirement states that X must be documented and the responsible entity has not documented X then the intent of the requirement has been missed and therefore the severity level must be severe. Similar conditions apply to any and all requirements that are binary in nature (i.e. the requirement is either met or not met) in that not meeting the requirement can only be a severe violation level. The impact on the BES would be taken care of by the violation risk factor. A documentation type of requirement would likely have a lower risk factor than a requirement for specific action (by the responsible entity) that impacts the BES.</p>				

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Martin Bauer	U.S. Bureau of Reclamation	5	Negative	<p>The CIP-003-2 R 2.3 Violation Level is characterized Severe for what appears to be failure to complete any one of the following requirements through the use of the "or": "A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; or changes to the delegated authority are not documented within thirty calendar days of the effective date." This characterization would not be consistent with other Severity Levels which would have been characterized Severe for failure to complete all the requirements.</p> <p>The CIP-003-2 R 2.4 Violation Level is characterized Severe when the senior manager failed to authorize exceptions. The language is ambiguous and can mean of no exceptions used were authorized or documented, or failure to even authorize one exception constitutes a severe violation. There is no allowance for the fact that there may be no exceptions or that no exceptions sought were authorized. The issue can only arise if the exception was implemented and not authorized. Language should read "The senior manager or delegate(s) did not authorize and document as required, one or more exceptions from the requirements of the cyber security policy as required that were invoked or implemented."</p>
<p>Response: Thank you for your comment. You have correctly identified an error in the Severe VSL. The drafting team has changed the word "or" to "and" for the recirculation ballot and will highlight this correction in the announcement for the recirculation ballot.</p> <p>Regarding the comments on CIP-003-2 R2.4, as defined, a VSL is an after the fact look at how well the responsible entity met the intent of the requirement. This is quite different from a violation risk factor which determines (if the requirement were to be violated) what would be the impact to the reliability of the bulk electric system. Further, the drafting team believes the current language, with "as required" at the end, allows for the situation where no exceptions have been sought.</p>				
Carter B Edge	SERC Reliability Corporation	10	Negative	<p>The posting material is so convoluted that I can't understand the specifics of what I am being asked to vote on. Not to mention that the posting indicates that this is an interpretation. If it is an interpretation where is the interpretation request? How is one to know the scope and reasoning for the changes without completely re-working the issue for themselves from version 1 to version 2 of the CIP standards? The drafting team should provide an overview or executive summary of thier work product and approach when asking for approval of such a disparate set of changes.</p>
<p>Response: Thank you for your comment. It appears this comment was meant for another project that was being balloted at the same time as the version 2 CIP standard VSLs.</p>				

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Voter	Entity	Segment	Vote	Comment	
Dana Cabbell	Southern California Edison Co.	1	Affirmative	<p>Although we understand that NERC stakeholders have recently approved a modification to the NERC Reliability Standards Development Procedure that will require that Violation Risk Factors and Violation Severity Levels be developed at the same time and by the same drafting team that drafts the respective underlying reliability standards, we would like you to consider the following recommendations for all future VRF and VSL projects:</p>	
David Schiada		3			<p>1. Concern: There appears to be an inconsistent gradation between reliability standards involving duration-based requirements. Many requirements in the various reliability standards require specific action prior to a defined elapsed time. The VSLs for all reliability standards appear to have inconsistencies when the requirement specifies an action within a defined elapsed time. Recommendation: We recommend enhancing the guideline(s) for VSL development to follow specific criteria for assigning severity level based on elapsed time. The VSLs may be based on some ratio/multiple of the original time stated in the requirement. For example, if a requirement specifies that an action be performed within 30 days, the VSL gradations might use 30 day increments: Lower - Action was performed within 31-60 days Moderate - Action was performed within 61-90 days High - An action was performed within 91-120 days Severe - Either action was not performed or it was performed >120 days.</p>
Marcus V Lotto		6			<p>2. Concern: There appears to be an inconsistency in the use of “binary” VSLs as opposed to “graded” VSLs. Because the decision as to whether a requirement is binary in nature is left to the various VSL drafting teams, it appears to be inconsistently applied. Some requirements that appear amenable to a graded approach have VSLs that are “binary” in nature. Recommendation: We recommend that the development of VSLs occur in conjunction with the development/revision of the respective standard. If the VSLs are developed in conjunction with the requirements, the requirements can be revised as needed to ensure compliance can be measured using the appropriate level. Additionally, we recommend more prescriptive guidance to VSL drafting teams surrounding the use of “binary” VSLs.</p>
				<p>3. Concern: There appears to be an inconsistent use of the “roll up” approach to assigning VSLs. Although the roll-up approach may be beneficial to avoid double jeopardy in some cases, it cannot be utilized in all instances of requirements containing sub-requirements. Since the decision to roll-up is left to the discretion of the various VSL drafting teams, it creates potential inconsistencies. Recommendation: We recommend that the development of VSLs occur in conjunction with the development/revision of the respective reliability standard. If the VSLs are developed in conjunction with the requirements, the requirements can be revised as needed to ensure compliance can be measured using the appropriate</p>	

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>level.</p> <p>4. Concern: There appears to be an inconsistent application of percentages in VSLs (i.e. 5% increments in some, but not all). Recommendation: We recommend that the guidelines for development of VSLs include the standardization of percentages, much like the quartiles in the existing VSL Development Guidelines Criteria. Additionally, the development of the VSLs should occur in conjunction with the development/revision of the respective reliability standards. If the VSLs are developed in conjunction with the requirements, the requirements can be revised as needed to ensure compliance can be measured using the appropriate level/gradation. Thank you for your attention to this matter.</p>
<p>Response: Thank you for your comment. The NERC standards development process has been modified to include the development of VSL by the Standards Drafting Team, as documented in the “Drafting Team Guidelines” Endorsed by the SC in its April 2009 revision. The document is available in the Standards Program area web site. NERC filed a proposal for modifying its approach to developing VSLs in August 2009, and this filing does address the issues you identified.</p>				
Guy V. Zito	Northeast Power Coordinating Council, Inc.	10	Affirmative	<p>The severe VSL for CIP003 R2.4 is as follows: The senior manager or delegate(s) did not authorize and document as required, any exceptions from the requirements of the cyber security policy as required. A future revision to the standard should consider a change to “existing” from “any” exceptions. “Any” implies that there must be at least one exception.</p>
<p>Response: Thank you for your comment. This comment will be forwarded to the version 4 CIP standards drafting team for their consideration when developing VSLs for the version 4 cyber security standards.</p>				
Terry Bilke	Midwest ISO, Inc.	2	Abstain	<p>We are turning the ballot over to another person and will cast our official position during recirculation.</p>
<p>Response: Thank you for your comment.</p>				

Standards Announcement Recirculation Ballot Window Open November 2–12, 2009

Now available at: <https://standards.nerc.net/CurrentBallots.aspx>

Project 2008-06: Cyber Security (VRFs and VSLs for Version 2 CIP Standards)

A recirculation ballot window for proposed Violation Severity Levels (VSLs) for critical infrastructure protection (CIP) standards CIP-002-2 through CIP-009-2 and Violation Risk Factors (VRFs) for CIP-003-2 and CIP-006-2 is now open **until 8 p.m. EST on November 12, 2009**.

Please note that the Severe VSL for CIP-003-2 Requirement R2.3 was modified to change “or” to “and” to correct an error. The edit is highlighted in yellow on page 5 of the redlined version. The edit is considered errata, allowing the project to proceed to this recirculation ballot.

Instructions

Members of the ballot pool associated with this project may log in and submit their votes from the following page: <https://standards.nerc.net/CurrentBallots.aspx>

Recirculation Ballot Process

The Standards Committee encourages all members of the ballot pool to review the consideration of comments submitted with the initial ballots. In the recirculation ballot, votes are counted by exception only — if a ballot pool member does not submit a revision to that member’s original vote, the vote remains the same as in the first ballot. Members of the ballot pool may:

- Reconsider and change their vote from the first ballot.
- Vote in the second ballot even if they did not vote on the first ballot.
- Take no action if they do not want to change their original vote.

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

Standards CIP-002-2 through CIP-009-2 have been approved by stakeholders; the purpose of this part of the project is to complete the VSLs and VRFs for those standards. This step is part of the overall Project 2008-06 — Cyber Security Order 706.

The posted VSLs are those associated with requirements that were modified when converting standards CIP-002-1 through CIP-009-1 into CIP-002-2 through CIP-009-2. The posted VRFs are for the two standards with VRF changes resulting from modifications made during the transition from standards CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2:

- CIP-003-2 — Security Management Controls
- CIP-006-2 — Physical Security of Critical Cyber Assets.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Standards Development Process

The [Reliability Standards Development Procedure](#) contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

*For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*

Note – this document only shows those VSLs that were changed as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2.

Following the initial ballot, the Severe VSL for CIP-003-2, Requirement R2.3 was modified to change “or” to “and” to correct an error in the VSLs. See yellow highlighted text on page 3.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards (Project 2008-06):

Index:

Standard Number CIP-002-2 Critical Cyber Asset Identification	2
Standard Number CIP-003-2 Security Management Controls	3
Standard Number CIP-004-2 Personnel & Training.....	5
Standard Number CIP-005-2 Electronic Security Perimeter(s).....	7
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....	8
Standard Number CIP-007-2 Systems Security Management.....	16
Standard Number CIP-008-2 Incident Reporting and Response Planning.....	19
Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets	20

Standard Number CIP-002-2 — Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1.	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.3.	N/A	N/A	<p>The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation,</p> <p>OR</p> <p>The document is not approved by the senior manager,</p> <p>OR</p> <p>Changes to the delegated authority are not documented within thirty calendar days of the effective date.</p>	<p>A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager;</p> <p>AND</p> <p>changes to the delegated authority are not documented within thirty calendar days of the effective date.</p>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 — Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.4.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3.2.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
R2.	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, implement, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1.	At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
R3.	N/A	The Responsible Entity has a personnel risk assessment	The Responsible Entity has a personnel risk assessment program	The Responsible Entity does not have a documented personnel risk

Standard Number CIP-004-2 — Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.</p>	<p>as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.</p>	<p>assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access.</p> <p>OR</p> <p>The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.</p>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 — Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3, Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.
R2.3.	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created and implemented but did not maintain a physical security plan.</p>	<p>The Responsible Entity did not document, implement, and maintain a physical security plan.</p>
R1.1.	N/A	<p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.</p>	<p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.</p>	<p>The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.</p> <p>OR</p> <p>Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to the Critical such Cyber Assets within the Electronic Security Perimeter.</p>

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.2.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
R1.6.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7.	N/A	N/A	The Responsible Entity's physical security plan addresses a process for updating the physical security plan within-thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or reconfiguration.
R1.8.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R1.9.	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
R3.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4.	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
R5.	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-2.
R6.	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. 	<p>method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. 	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. 	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
R7.	The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained physical access logs for less than 45 calendar days.
R8.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2,	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.

Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	and R8.3.	R8.3.	R8.3.	

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement) , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1.	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.</p>
R5.1.3.	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.</p>
R7.	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not maintain</p>	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address redeployment as specified in R7.2.</p>	<p>The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1.</p>	<p>The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.</p>

Standard Number CIP-007-2 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	records as specified in R7.3.			
R9.	N/A	N/A	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.</p>

Standard Number CIP-008-2 — Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

Standard Number CIP-009-2 — Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 30 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

Note – this document only shows those VSLs that were changed as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2.

[Following the initial ballot, the Severe VSL for CIP-003-2, Requirement R2.3 was modified to change “or” to “and” to correct an error in the VSLs. See yellow highlighted text on page 5.](#)

**Proposed Violation Severity Levels for the CIP
 Version 2 Series of Standards (Project 2008-06):**

Index:

Standard Number CIP-002-2 Critical Cyber Asset Identification	2
Standard Number CIP-003-2 Security Management Controls	443
Standard Number CIP-004-2 Personnel & Training.....	776
Standard Number CIP-005-2 Electronic Security Perimeter(s).....	11110
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....	131312
Standard Number CIP-007-2 Systems Security Management.....	272726
Standard Number CIP-008-2 Incident Reporting and Response Planning.....	323231
Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets	333332

Standard Number CIP-002-2 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4. (Version 1)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
R4 (Proposed changes to align with version 2)	N/A	N/A <u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)</u>	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.) <u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)</u>	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both two or more of the following: the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) <u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)</u>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	N/A	N/A	The Responsible Entity has not assigned a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2.1. (Version 1)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
R2.3. (Version 1)	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exception from the requirements of the cyber security policy as required.

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.3 (Proposed changes to align with version 2)	N/A N/A		<p>N/A</p> <p><u>The identification of a senior manager's delegate does not include at least one of the following: name, title, or date of the designation.</u></p> <p><u>OR</u></p> <p><u>The document is not approved by the senior manager.</u></p> <p><u>OR</u></p> <p><u>Changes to the delegated authority are not documented within thirty calendar days of the effective date.</u></p>	<p>A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager;</p> <p>or</p> <p>AND</p> <p>changes to the delegated authority are not documented within thirty calendar days of the effective date.</p>
New R2.4 (Proposed to align with version 2)	N/A	N/A	N/A	<p>The senior manager or delegate(s) did not authorize and document as required, <u>any</u> exceptions from the requirements of the cyber security policy <u>as required</u>.</p>

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-003-2 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.2. (Version 1)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.
R3.2 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include either : 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include both : 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
R1 (Proposed changes to align with version 2)	The Responsible Entity established, (implemented) , and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, (implement) , nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, (implement) , maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
R2. (Version 1)	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Proposed changes to align with version 2)	The Responsible Entity established _(implemented)_ and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish _(implement)_ nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish _(implement)_ , maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1. (Version 1)	At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.	15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.
R2.1 (Proposed changes to align with version 2)	At least one individual but less than 5% of personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	At least 5% but less than 10% of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	At least 10% but less than 15% of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.	15% or more of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency within ninety calendar days of such authorization.

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3. (Version 1)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in sixty (60) days or more of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.
R3 (Proposed changes to align with version 2)	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after in sixty (60) days or more of such personnel were being granted such access except in specified circumstances such as an emergency.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-004-2 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5. (Version 1)	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
R1.5 (Proposed changes to align with version 2)	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3, Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-2;; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3;; Standard CIP-006-2 Requirements R2 and R3;; Standard CIP-007-2, Requirements R1 and R3 through R9;; Standard CIP-008-2;; and Standard CIP-009-2.
R2.3. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not maintain a procedure for securing dial-up access to the Electronic

Proposed Violation Severity Levels for the CIP Version 2 Series of Standards

Standard Number CIP-005-2 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Security Perimeter(s) where applicable.
R2.3 (Proposed changes to align with version 2)	N/A	N/A	N/A The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement <u>nor</u> maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created but did not maintain a physical security plan.</p>	The Responsible Entity did not create and maintain a physical security plan.
R1 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created and implemented but did not maintain a physical security plan.</p>	The Responsible Entity did not create and document, implement, and maintain a physical security plan.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.1. (Version 1)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical Cyber Assets.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical Cyber Assets.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical access to the Critical Cyber Assets.
R1.1 (Proposed changes to align with version 2)	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical such Cyber Assets <u>within the Electronic Security Perimeter</u> .	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical such Cyber Assets <u>within the Electronic Security Perimeter</u> .	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not deployed and documented alternative measures to control physical to the Critical-such Cyber Assets within the Electronic Security Perimeter .
R1.2. (Version 1)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify all access points through each Physical Security Perimeter but not measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.2 (Proposed changes to align with version 2)	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.4 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the appropriate use of physical access controls as described in Requirement R3.
R1.4 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the address the appropriate use of physical access controls as described in

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R3 R4.
R1.5 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan does not include either the procedures for reviewing access authorization requests or revocation of access authorization, in accordance with CIP-004 Requirement R4.	The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
R1.5 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan does not include address either the procedures process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	The Responsible Entity's physical security plan does not include address the process procedures for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
R1.6 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for escorted access within the physical security perimeter.
R1.6 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures address the process for continuous escorted access within the physical security perimeter.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.7 (Version 1)	N/A	N/A	The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration but the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.
R1.7 (Proposed changes to align with version 2)	N/A	N/A	The Responsible Entity's physical security plan includes addresses a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within 90 thirty calendar days of the completion of any physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not include address a process for updating the physical security plan within ninety thirty calendar days of the completion of any physical security system redesign or reconfiguration.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.8 (Version 1)	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but one (1) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but two (2) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is provided all but three (3) of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is not provided four (4) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.
R1.8 (Proposed changes to align with version 2)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Version 1)	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include a process for ensuring that the physical security plan is reviewed at least annually.
R1.9 (Proposed changes to align with version 2)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)	(Deleted – remove VSL.)

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2 (Version 1)	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.
R2 (Proposed changes to align with version 2)	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
New R2.1 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
New R2.2 (Proposed changes to align with version 2)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)	N/A (Rolled up into R2.)
R3 (Version 1)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirements R3.1 or R3.2.	Requirements R3.1 or R3.2.	OR One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.
R3 (Proposed changes to align with version 2)	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4 (Version 1)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4 (Proposed changes to align with version 2)	N/A	<p>The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	<p>The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5 (Version 1)	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs for at least ninety calendar days.
R5 (Proposed changes to align with version 2)	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. <p>OR</p> <p>An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-</p>

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				008-2.
R6 (Version 1)	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include one of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include two of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly but the program does not include any of the requirements R6.1, R6.2, and R6.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.
R6 (Proposed changes to align with version 2)	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record 	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by 	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of 	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
<p>New R7 (Proposed changes to align with version 2)</p>	<p>of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.</p> <p><u>The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.</u> N/A</p>	<p>security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.</p> <p><u>The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.</u> N/A</p>	<p>physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.</p> <p><u>The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.</u> N/A</p>	<p>physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.</p> <p><u>The Responsible Entity retained physical access logs for less than 45 calendar days.</u> The Responsible Entity did not retain electronic access logs in accordance with the requirements of Standard CIP-008-2.</p>
<p>New R8 (Proposed changes to align with version 2)</p>	<p>The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.</p>	<p>The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.</p>	<p>The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.</p>	<p>The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.</p>
<p>New R8.1 (Proposed changes to align with</p>	<p>N/A (Rolled up into R8.)</p>	<p>N/A (Rolled up into R8.)</p>	<p>N/A (Rolled up into R8.)</p>	<p>N/A (Rolled up into R8.)</p>

Standard Number CIP-006-2 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
version 2)				
New R8.2 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)
New R8.3 (Proposed changes to align with version 2)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)	N/A (Rolled up into R8.)

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2. (Version 1)	N/A	The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2 (Proposed changes to align with version 2)	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. (Version 1)	The Responsible Entity established and documented, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established but did not document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish nor document , either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3 (Proposed changes to	The Responsible Entity established (implemented) and documented, either separately or	The Responsible Entity established (implemented) but did not document , either	The Responsible Entity documented but did not establish (implement) , either	The Responsible Entity did not establish (implement) nor document , either separately or as

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
align with version 2)	as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R4.1. (Version 1)	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1 (Proposed changes to align with version 2)	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</p> <p>OR</p> <p>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.</p>
R5.1.3. (Version 1)	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.</p>
R5.1.3 (Proposed changes to align with version 2)	N/A	N/A	N/A	<p>The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.</p>

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R7. (Version 1)	The Responsible Entity established formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not maintain records as specified in R7.3.	The Responsible Entity established formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address redeployment as specified in R7.2.	The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R7 (Proposed changes to align with version 2)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not maintain records as specified in R7.3.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.
R9 (Version 1)	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually or the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.

Standard Number CIP-007-2 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R9 (Proposed changes to align with version 2)	N/A	N/A	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually.</p> <p>OR</p> <p>or the The Responsible Entity did not document Cchanges resulting from modifications to the systems or controls within thirty ninety calendar days of the change being completed.</p>	<p>The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were Cchanges resulting from modifications to the systems or controls documented within thirty ninety calendar days of the change being completed.</p>

Standard Number CIP-008-2 Incident Reporting and Response Planning				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1. (Version 1)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6	The Responsible Entity has not developed a Cyber Security Incident response plan.
R1 (Proposed changes to align with version 2)	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3 (Version 1)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.
R3 (Proposed changes to align with version 2)	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 90	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery

Standard Number CIP-009-2 Recovery Plans for Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	30 but less than or equal to 120 calendar days of the change.	than or equal to 150 calendar days of the change.	than or equal to 180 calendar days of the change.	plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2. Only the 15 VRFs shown in red text are “new.” There were no changes to these VRFs based on stakeholder comments.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 2 CIP-002-2 thru CIP-009-2 Standards:

Index:

Standard Number CIP-003-2 Security Management Controls2
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....3

Standard Number CIP-003 — Security Management Controls			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.	LOWER
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2 R2.3.		Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2 R2.4.		The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8.	Annual review of the physical security plan.	LOWER
CIP-006-2	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM
CIP-006-2	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-2	R4.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets 	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used: <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been 	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		<p>opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.</p> <ul style="list-style-type: none"> Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	
CIP-006-2	R6.	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4 	LOWER
CIP-006-2	R7.	<p>Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.</p>	LOWER
CIP-006-2	R8.	<p>Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:</p>	MEDIUM
CIP-006-2	R8.1.	<p>Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.</p>	MEDIUM
CIP-006-2	R8.2.	<p>Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.</p>	LOWER
CIP-006-2	R8.3.	<p>Retention of outage records regarding access controls, logging, and monitoring for a</p>	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		minimum of one calendar year.	

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition from CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2. Only the 15 VRFs shown in red text are “new.” There were no changes to these VRFs based on stakeholder comments.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 2 CIP-002-2 thru CIP-009-2 Standards:

Index:

Standard Number CIP-003-2 Security Management Controls2
Standard Number CIP-006-2 Physical Security of Critical Cyber Assets.....3

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-003 — Security Management Controls			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.	LOWER
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2	R2.3. (New)	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2	R2.4. (New – similar to version 1 R2.3 which was LOWER)	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8. (New – similar to version 1 R1.9 which was LOWER)	Annual review of the physical security plan.	LOWER
CIP-006-2	R2. (New)	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers,	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
		shall:	
CIP-006-2	R2.1. (New)	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2. (New)	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM
CIP-006-2	R3. (New)	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-2	R4. (New – Similar to version 1 R2, R2.1, R2.2, R2.3, and R2.4 combined – which were all MEDIUM)	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets 	MEDIUM
CIP-006-2	R5. (New – Similar to version 1 R3, R3.1, and R3.2 combined – R3)	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring	MEDIUM

Proposed Violation Risk Factors for the CIP Version 2 Series of Standards

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
	and R3.1 were MEDIUM and R3.2 was LOWER)	<p>methods shall be used:</p> <ul style="list-style-type: none"> Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 	
CIP-006-2	R6. (New – Similar to version 1 R4, R4.1, R4.2, and R4.3 combined – which were all LOWER)	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4 	LOWER
CIP-006-2	R7. New – Similar to version 1 R5 – which was LOWER)	<p>Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.</p>	LOWER
CIP-006-2	R8. (New – Similar to version 1 R6 – which was MEDIUM)	<p>Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:</p>	MEDIUM
CIP-006-2	R8.1.	<p>Testing and maintenance of all physical security mechanisms on a cycle no longer than</p>	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	Requirement Number	Text of Requirement	Violation Risk Factor
	(New – Similar to version 1 R6.1 – which was MEDIUM)	three years.	
CIP-006-2	R8.2. (New – Similar to version 1 R6.2 – which was LOWER)	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-2	R8.3. (New – Similar to version 1 R6.3 – which was LOWER)	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER

Standards Announcement Final Ballot Results

Now available at: <https://standards.nerc.net/Ballots.aspx>

Project 2008-06: Cyber Security (VRFs and VSLs for Version 2 CIP Standards)

The recirculation ballot for proposed Violation Severity Levels (VSLs) for critical infrastructure protection (CIP) standards CIP-002-2 through CIP-009-2 and Violation Risk Factors (VRFs) for CIP-003-2 and CIP-006-2 ended November 12, 2009.

Ballot Results

Voting statistics are listed below, and the [Ballot Results](#) Web page provides a link to the detailed results:

Quorum: 88.70%
Approval 94.24%

The ballot pool approved the VSLs and VRFs. Ballot criteria details are listed at the end of the announcement.

Next Steps

The VSLs and VRFs will be submitted to the NERC Board of Trustees for approval.

Project Background

Standards CIP-002-2 through CIP-009-2 have been approved by stakeholders; the purpose of this part of the project is to complete the VSLs and VRFs for those standards. This step is part of the overall Project 2008-06 — Cyber Security Order 706.

The VSLs are those associated with requirements that were modified when converting standards CIP-002-1 through CIP-009-1 into CIP-002-2 through CIP-009-2. The VRFs are for the two standards with VRF changes resulting from modifications made during the transition from standards CIP-002-1 through CIP-009-1 to CIP-002-2 through CIP-009-2:

- CIP-003-2 — Security Management Controls
- CIP-006-2 — Physical Security of Critical Cyber Assets.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Standards Development Process

The [Reliability Standards Development Procedure](#) contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Ballot Criteria

Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

User Name

Password

Log in

Register

- Ballot Pools
- Current Ballots
- Ballot Results
- Registered Ballot Body
- Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Cyber Security (VRFs and VSLs for Version 2 CIP Standards)_rc
Ballot Period:	11/2/2009 - 11/12/2009
Ballot Type:	recirculation
Total # Votes:	212
Total Ballot Pool:	239
Quorum:	88.70 % The Quorum has been reached
Weighted Segment Vote:	94.24 %
Ballot Results:	The Standard has Passed

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain # Votes	No Vote
			# Votes	Fraction	# Votes	Fraction		
1 - Segment 1.	63	1	45	0.882	6	0.118	8	4
2 - Segment 2.	9	0.7	7	0.7	0	0	2	0
3 - Segment 3.	54	1	41	0.953	2	0.047	6	5
4 - Segment 4.	14	1	9	0.9	1	0.1	1	3
5 - Segment 5.	44	1	28	0.933	2	0.067	8	6
6 - Segment 6.	33	1	22	1	0	0	4	7
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	9	0.7	7	0.7	0	0	0	2
9 - Segment 9.	8	0.6	6	0.6	0	0	2	0
10 - Segment 10.	5	0.5	4	0.4	1	0.1	0	0
Totals	239	7.5	169	7.068	12	0.432	31	27

Individual Ballot Pool Results

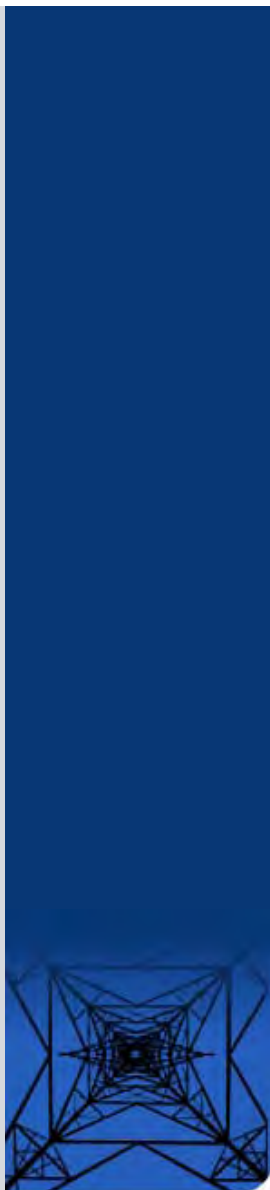
Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Abstain	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	

1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	City Utilities of Springfield, Missouri	Jeff Knottek		
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	E.ON U.S. LLC	Larry Monday		
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Albert Poire	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Negative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Kissimmee Utility Authority	Joe B Watson	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	Rodney Hawkins	Negative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	National Grid	Manuel Couto	Affirmative	
1	Nebraska Public Power District	Richard L. Koch		
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	Ohio Valley Electric Corp.	Robert Matthey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Oncor Electric Delivery	Charles W. Jenkins	Abstain	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Negative	
1	PP&L, Inc.	Ray Mammarella	Abstain	
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Abstain	
1	SaskPower	Wayne Guttormson	Abstain	
1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Abstain	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	View
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Affirmative	
1	Southwestern Power Administration	Gary W Cox	Affirmative	
1	Tampa Electric Co.	Thomas J. Szelistowski	Abstain	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Jason L. Murray	Abstain	
2	BC Transmission Corporation	Faramarz Amjadi	Affirmative	
2	California ISO	Greg Tillitson	Abstain	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Affirmative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Affirmative	

3	Allegheny Power	Bob Reeping	Affirmative	
3	American Electric Power	Raj Rana	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Power Agency	Duane S. Dahlquist	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Farmington	Linda R. Jacobson	Affirmative	
3	City of Lansing by its Board of Water and Light	David C Bolan		
3	City Public Service of San Antonio	Edwin Les Barrow	Affirmative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Abstain	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W. Pourciau	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Affirmative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory David Woessner	Negative	
3	Lakeland Electric	Mace Hunter	Abstain	
3	Lincoln Electric System	Bruce Merrill		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Abstain	
3	Manitoba Hydro	Greg C Parent	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscataine Power & Water	John Bos	Affirmative	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters		
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	Zack Dusenbury	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	View
3	Tampa Electric Co.	Ronald L. Donahey		
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt		
4	City of Troy Utilities	Brian M Chandler		
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Northern California Power Agency	Fred E. Young	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	

4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Abstain	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Consolidated Edison Co. of New York	Edwin E Thompson	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Robert Smith	Affirmative	
5	Edison Mission Energy	Ellen Oswald	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner		
5	FPL Energy	Benjamin Church		
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	JEA	Donald Gilbert	Abstain	
5	Kansas City Power & Light Co.	Scott Heidtbrink		
5	Lakeland Electric	Thomas J Trickey	Negative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Louisville Gas and Electric Co.	Charlie Martin	Abstain	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Abstain	
5	Orlando Utilities Commission	Richard Kinan	Negative	View
5	PacifiCorp Energy	David Godfrey	Abstain	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PPL Generation LLC	Mark A. Heimbach	Abstain	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
5	RRI Energy	Thomas J. Bradish	Affirmative	
5	Sacramento Municipal Utility District	Bethany Wright	Affirmative	
5	Salt River Project	Glen Reeves	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Southeastern Power Administration	Douglas Spencer	Abstain	
5	Tampa Electric Co.	Frank L Busot	Abstain	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	View
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Chris Lyons	Abstain	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Eugene Water & Electric Board	Daniel Mark Bedbury		
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell		
6	Great River Energy	Donna Stephenson		
6	Kansas City Power & Light Co.	Thomas Saitta	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Louisville Gas and Electric Co.	Daryn Barker	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PacifiCorp	Gregory D Maxfield	Affirmative	

6	Portland General Electric Co.	John Jamieson	Affirmative	
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson	Affirmative	
6	Salt River Project	Mike Hummel	Affirmative	
6	Santee Cooper	Suzanne Ritter	Abstain	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Southern California Edison Co.	Marcus V Lotto	Affirmative	View
6	Tampa Electric Co.	Joann Wehle		
6	Western Area Power Administration - UGP Marketing	John Stonebarger		
6	Xcel Energy, Inc.	David F. Lemmons	Abstain	
8	Dennis Neitzel	Dennis Neitzel	Affirmative	
8	Edward C Stein	Edward C Stein	Affirmative	
8	Encari	Matthew E. Luallen		
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz	Affirmative	
8	Volkman Consulting, Inc.	Terry Volkman	Affirmative	
8	Wally Magda	Wally Magda	Affirmative	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	Maine Public Utilities Commission	Jacob A McDermott	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Service Commission of South Carolina	Philip Riley	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	View
10	ReliabilityFirst Corporation	Jacqui Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Negative	View
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	



Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
 Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

[Account Log-In/Register](#)

Copyright © 2008 by the North American Electric Reliability Corporation. : All rights reserved.
 A New Jersey Nonprofit Corporation

Exhibit C

**CIP Version 2 Violation Severity Level and Violation Risk Factor Drafting
Team Roster**

Cyber Security Violation Severity Levels Drafting Team (Project 2008-14)

Chairman	Larry Bugh Chief Security Officer	ReliabilityFirst Corporation 320 Springside Drive — Suite 300 Akron, Ohio 44333	(330) 247-3046 (330) 456-3648 Fx larry.bugh@rfirst.org
	Jonathan Bransky IT Security Manager	Public Service Enterprise Group Incorporated 80 Park Plaza — T-16 Newark, New Jersey 07102	(973) 430-6294 jonathan.bransky@ pseg.com
	David Dunn	Independent Electricity System Operator Station A, Box 4474 Toronto, Ontario M5W 4E5	905.855.6286 david.dunn@ ieso.ca
	Mark A. Engels Director - IT Risk Management	Dominion Virginia Power P.O. Box 26666 Richmond, Virginia 23261	(804) 775-5263 (804) 771-3067 Fx mark.engels@dom.com
	Michael Mertz Project Manager - Regulatory Compliance	Southern California Edison Co. 4910 Rivergrade Road Irwindale, California 91706	(626) 543-6104 (626) 862-9110 Fx Michael.Mertz@sce.com
	James W. Sample Director of Cyber Security	Tennessee Valley Authority 1101 Market Street Mailstop: SP 5A-C Chattanooga, Tennessee 37402-2801	(423) 751-4794 (423) 751-6858 Fx jwsample@tva.gov
	William Souza Manager, Security Integration	PJM Interconnection, L.L.C. 955 Jefferson Avenue Norristown, Pennsylvania 19403	(610) 666-2237 (610) 728-4855 Fx beknh03@gmail.com
NERC Coordinator	Al Calafiore Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx al.calafiore@nerc.net
NERC Staff	Scott R. Mix Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx scott.mix@nerc.net

Exhibit D

Complete Matrix of Violation Severity Levels for Approved Reliability Standards

Complete Violation Severity Levels Matrix
Encompassing All Commission-Approved Reliability Standards

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-001-0.1a	R1.	Each Balancing Authority shall operate such that, on a rolling 12-month basis, the average of the clock-minute averages of the Balancing Authority's Area Control Error (ACE) divided by 10B (B is the clock-minute average of the Balancing Authority Area's Frequency Bias) times the corresponding clock-minute averages of the Interconnection's Frequency Error is less than a specific limit. This limit is a constant derived from a targeted frequency bound (separately calculated for each Interconnection) that is reviewed and set as necessary by the NERC Operating Committee. <i>See Standard for Formula.</i>	The Balancing Authority Area's value of CPS1 is less than 100% but greater than or equal to 95%.	The Balancing Authority Area's value of CPS1 is less than 95% but greater than or equal to 90%.	The Balancing Authority Area's value of CPS1 is less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS1 is less than 85%.
BAL-001-0.1a	R2.	Each Balancing Authority shall operate such that its average ACE for at least 90% of clock-ten-minute periods (6 non-overlapping periods per hour) during a calendar month is within a specific limit, referred to as L ₁₀ . <i>See Standard for Formula.</i>	The Balancing Authority Area's value of CPS2 is less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS2 is less than 85% but greater than or equal to 80%.	The Balancing Authority Area's value of CPS2 is less than 80% but greater than or equal to 75%.	The Balancing Authority Area's value of CPS2 is less than 75%.
BAL-001-0.1a	R3.	Each Balancing Authority providing Overlap Regulation Service shall evaluate	N/A	N/A	N/A	The Balancing Authority providing Overlap Regulation

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirement R1 (i.e., Control Performance Standard 1 or CPS1) and Requirement R2 (i.e., Control Performance Standard 2 or CPS2) using the characteristics of the combined ACE and combined Frequency Bias Settings.				Service failed to use a combined ACE and frequency bias.
BAL-001-0.1a	R4.	Any Balancing Authority receiving Overlap Regulation Service shall not have its control performance evaluated (i.e. from a control performance perspective, the Balancing Authority has shifted all control requirements to the Balancing Authority providing Overlap Regulation Service).	N/A	N/A	N/A	The Balancing Authority receiving Overlap Regulation Service failed to ensure that control performance was being evaluated in a manner consistent with the calculation methodology as described in BAL-001-01 R3.
BAL-002-0	R1.	Each Balancing Authority shall have access to and/or operate Contingency Reserve to respond to Disturbances. Contingency Reserve may be supplied from generation, controllable load resources, or coordinated adjustments to Interchange Schedules.	N/A	N/A	N/A	The Balancing Authority does not have access to and/or operate Contingency Reserve to respond to Disturbances.
BAL-002-0	R1.1.	A Balancing Authority may elect to fulfill its Contingency Reserve obligations by participating as a member of a Reserve Sharing Group. In such cases, the Reserve Sharing Group shall have the	N/A	N/A	N/A	The Balancing Authority has elected to fulfill its Contingency Reserve obligations by participating as a member of a Reserve

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		same responsibilities and obligations as each Balancing Authority with respect to monitoring and meeting the requirements of Standard BAL-002.				Sharing Group and the Reserve Sharing Group has not provided the same responsibilities and obligations as required of the responsible entity with respect to monitoring and meeting the requirements of Standard BAL-002.
BAL-002-0	R2.	Each Regional Reliability Organization, sub-Regional Reliability Organization or Reserve Sharing Group shall specify its Contingency Reserve policies, including:	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 1 of the following sub-requirements.	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 2 or 3 of the following sub-requirements.	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 4 or 5 of the following sub-requirements.	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify all 6 of the following sub-requirements.
BAL-002-0	R2.1.	The minimum reserve requirement for the group.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the minimum reserve requirement for the group.
BAL-002-0	R2.2.	Its allocation among members.	N/A	N/A	N/A	The Regional Reliability Organization, sub-

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Regional Reliability Organization, or Reserve Sharing Group has failed to specify the allocation of reserves among members.
BAL-002-0	R2.3.	The permissible mix of Operating Reserve – Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the permissible mix of Operating Reserve – Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.
BAL-002-0	R2.4.	The procedure for applying Contingency Reserve in practice.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to provide the procedure for applying Contingency Reserve in practice.
BAL-002-0	R2.5.	The limitations, if any, upon	N/A	N/A	N/A	The Regional

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the amount of interruptible load that may be included.				Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the limitations, if any, upon the amount of interruptible load that may be included.
BAL-002-0	R2.6.	The same portion of resource capacity (e.g., reserves from jointly owned generation) shall not be counted more than once as Contingency Reserve by multiple Balancing Authorities.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has allowed the same portion of resource capacity (e.g., reserves from jointly owned generation) to be counted more than once as Contingency Reserve by multiple Balancing Authorities.
BAL-002-0	R3.	Each Balancing Authority or Reserve Sharing Group shall activate sufficient Contingency Reserve to comply with the DCS.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than 100% but greater than or equal to 95%.	less than 95% but greater than or equal to 90%.	less than 90% but greater than or equal to 85%.	less than 85%.
BAL-002-0	R3.1.	As a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency. All Balancing Authorities and Reserve Sharing Groups shall review, no less frequently than annually, their probable contingencies to determine their prospective most severe single contingencies.	The Balancing Authority or Reserve Sharing Group failed to review their probable contingencies to determine their prospective most severe single contingencies annually.	N/A	N/A	The Balancing Authority or Reserve Sharing Group failed to carry at least enough Contingency Reserve to cover the most severe single contingency.
BAL-002-0	R4.	A Balancing Authority or Reserve Sharing Group shall meet the Disturbance Recovery Criterion within the Disturbance Recovery Period for 100% of Reportable Disturbances. The Disturbance Recovery Criterion is:	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 90% and less than 100% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 80% and less than or equal to 90% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 70% and less than or equal to 80% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 0% and less than or equal to 70% of Reportable Disturbances.
BAL-002-0	R4.1.	A Balancing Authority shall return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to zero. For negative initial ACE values just prior to the Disturbance, the Balancing Authority shall	N/A	N/A	N/A	The Balancing Authority failed to return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		return ACE to its pre-Disturbance value.				zero or for negative initial ACE values failed to return ACE to its pre-Disturbance value.
BAL-002-0	R4.2.	The default Disturbance Recovery Period is 15 minutes after the start of a Reportable Disturbance. This period may be adjusted to better suit the needs of an Interconnection based on analysis approved by the NERC Operating Committee.	N/A	N/A	N/A	N/A
BAL-002-0	R5.	Each Reserve Sharing Group shall comply with the DCS. A Reserve Sharing Group shall be considered in a Reportable Disturbance condition whenever a group member has experienced a Reportable Disturbance and calls for the activation of Contingency Reserves from one or more other group members. (If a group member has experienced a Reportable Disturbance but does not call for reserve activation from other members of the Reserve Sharing Group, then that member shall report as a single Balancing Authority.) Compliance may be demonstrated by either of the following two methods:	The Reserve Sharing Group met the DCS requirement for more than 90% and less than 100% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 80% and less than or equal to 90% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 70% and less than or equal to 80% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 0% and less than or equal to 70% of Reportable Disturbances.
BAL-002-0	R5.1.	The Reserve Sharing Group	N/A	N/A	N/A	N/A

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reviews group ACE (or equivalent) and demonstrates compliance to the DCS. To be in compliance, the group ACE (or its equivalent) must meet the Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.				
BAL-002-0	R5.2.	The Reserve Sharing Group reviews each member's ACE in response to the activation of reserves. To be in compliance, a member's ACE (or its equivalent) must meet the Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.	N/A	N/A	N/A	N/A
BAL-002-0	R6.	A Balancing Authority or Reserve Sharing Group shall fully restore its Contingency Reserves within the Contingency Reserve Restoration Period for its Interconnection.	The Balancing Authority or Reserve Sharing Group restored less than 100% but greater than 90% of its contingency reserves during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than or equal to 90% but greater than 80% of its contingency reserves during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than or equal to 80% but greater than or equal to 70% of its Contingency Reserve during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than 70% of its Contingency Reserves during the Contingency Reserve Restoration Period.
BAL-002-0	R6.1.	The Contingency Reserve	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Restoration Period begins at the end of the Disturbance Recovery Period.				
BAL-002-0	R6.2.	The default Contingency Reserve Restoration Period is 90 minutes. This period may be adjusted to better suit the reliability targets of the Interconnection based on analysis approved by the NERC Operating Committee.	N/A	N/A	N/A	N/A
BAL-003-0.1b	R1.	Each Balancing Authority shall review its Frequency Bias Settings by January 1 of each year and recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.	N/A	N/A	The Balancing Authority reviewed its Frequency Bias Settings prior January 1, but failed to recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.	The Balancing Authority failed to review its Frequency Bias Settings prior to January 1, and failed to recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.
BAL-003-0.1b	R1.1.	The Balancing Authority may change its Frequency Bias Setting, and the method used to determine the setting, whenever any of the factors used to determine the current bias value change.	N/A	N/A	N/A	The Balancing Authority changed its Frequency Bias Setting by changing the method used to determine the setting, without any of the factors used to determine the current bias value changing.
BAL-003-0.1b	R1.2.	Each Balancing Authority shall report its Frequency Bias Setting, and method for	The Balancing Authority has not reported its method	The Balancing Authority has not reported its	The Balancing Authority has not reported its method	The Balancing Authority has failed to report as directed

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		determining that setting, to the NERC Operating Committee.	for calculating frequency bias setting.	frequency bias setting.	for calculating frequency bias and has not reported its frequency bias setting.	by the requirement.
BAL-003-0.1b	R2.	Each Balancing Authority shall establish and maintain a Frequency Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response. Frequency Bias may be calculated several ways:	N/A	N/A	N/A	The Balancing Authority established and maintained a Frequency Bias Setting that was less than, the Balancing Authority's Frequency Response.
BAL-003-0.1b	R2.1.	The Balancing Authority may use a fixed Frequency Bias value which is based on a fixed, straight-line function of Tie Line deviation versus Frequency Deviation. The Balancing Authority shall determine the fixed value by observing and averaging the Frequency Response for several Disturbances during on-peak hours.	N/A	N/A	N/A	The Balancing Authority determination of the fixed Frequency Bias value was not based on observations and averaging the Frequency Response from Disturbances during on-peak hours.
BAL-003-0.1b	R2.2.	The Balancing Authority may use a variable (linear or non-linear) bias value, which is based on a variable function of Tie Line deviation to Frequency Deviation. The Balancing Authority shall determine the variable frequency bias value by analyzing Frequency Response	N/A	N/A	N/A	The Balancing Authorities variable frequency bias maintained was not based on an analyses of Frequency Response as it varied with factors such as load, generation, governor

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		as it varies with factors such as load, generation, governor characteristics, and frequency.				characteristics, and frequency.
BAL-003-0.1b	R3.	Each Balancing Authority shall operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, unless such operation is adverse to system or Interconnection reliability.	N/A	N/A	N/A	The Balancing Authority did not operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, during periods when such operation would not have been adverse to system or Interconnection reliability.
BAL-003-0.1b	R4.	Balancing Authorities that use Dynamic Scheduling or Pseudo-ties for jointly owned units shall reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting.	N/A	N/A	N/A	The Balancing Authority that used Dynamic Scheduling or Pseudo-ties for jointly owned units did not reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting.
BAL-003-0.1b	R4.1.	Fixed schedules for Jointly Owned Units mandate that Balancing Authority (A) that contains the Jointly Owned Unit must incorporate the respective share of the unit governor droop response for any Balancing Authorities that	N/A	N/A	N/A	The Balancing Authority (A) that contained the Jointly Owned Unit with fixed schedules did not incorporate the respective share of the unit governor

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		have fixed schedules (B and C). See the diagram below.				droop response for any Balancing Authorities that have fixed schedules (B and C).
BAL-003-0.1b	R4.2.	The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit shall not include their share of the governor droop response in their Frequency Bias Setting. <i>See Standard for Graphic</i>	N/A	N/A	N/A	The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit, included their share of the governor droop response in their Frequency Bias Setting.
BAL-003-0.1b	R5.	Balancing Authorities that serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change.	N/A	N/A	N/A	The Balancing Authority that served native load failed to have a monthly average Frequency Bias Setting that was at least 1% of the entities estimated yearly peak demand per 0.1 Hz change.
BAL-003-0.1b	R5.1.	Balancing Authorities that do not serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.	N/A	N/A	N/A	The Balancing Authority that does not serve native load did not have a monthly average Frequency Bias Setting that was at least 1% of its estimated maximum generation level in

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the coming year per 0.1 Hz change.
BAL-003-0.1b	R6.	A Balancing Authority that is performing Overlap Regulation Service shall increase its Frequency Bias Setting to match the frequency response of the entire area being controlled. A Balancing Authority shall not change its Frequency Bias Setting when performing Supplemental Regulation Service.	N/A	The Balancing Authority that was performing Overlap Regulation Service changed its Frequency Bias Setting while performing Supplemental Regulation Service.	The Balancing Authority that was performing Overlap Regulation Service failed to increase its Frequency Bias Setting to match the frequency response of the entire area being controlled.	N/A
BAL-004-0	R.3.2.	The Balancing Authority shall offset its Net Interchange Schedule (MW) by an amount equal to the computed bias contribution during a 0.02 Hertz Frequency Deviation (i.e. 20% of the Frequency Bias Setting).	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 0 to 25% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 25 to 50% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 50 to 75% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 75% or more of the time error corrections.
BAL-004-0	R1.	Only a Reliability Coordinator shall be eligible to act as Interconnection Time Monitor. A single Reliability Coordinator in each Interconnection shall be designated by the NERC Operating Committee to serve as Interconnection Time Monitor.	N/A	N/A	N/A	The responsible entity has designated more than one interconnection time monitor for a single interconnection.
BAL-004-0	R2.	The Interconnection Time Monitor shall monitor Time	N/A	N/A	N/A	The RC serving as the Interconnection

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Error and shall initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.				Time Monitor failed to initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.
BAL-004-0	R3.	Each Balancing Authority, when requested, shall participate in a Time Error Correction by one of the following methods:	The Balancing Authority participated in more than 75% and less than 100% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in more than 50% and less than or equal to 75% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in more than 25% and less than or equal to 50% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in less than or equal to 25% of requested Time Error Corrections for the calendar year.
BAL-004-0	R3.1.	The Balancing Authority shall offset its frequency schedule by 0.02 Hertz, leaving the Frequency Bias Setting normal; or	The Balancing Authority failed to offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 0 to 25% of the time error corrections for the year.	The Balancing Authority failed to offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 25 to 50% of the time error corrections for the year.	The Balancing Authority failed to offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 50 to 75% of the time error corrections for the year.	The Balancing Authority failed to offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 75% or more of the time error corrections for the year.
BAL-004-0	R4.	Any Reliability Coordinator in an Interconnection shall have the authority to request the Interconnection Time Monitor to terminate a Time Error Correction in progress, or a scheduled Time Error Correction that has not begun, for reliability considerations.	N/A	N/A	N/A	The RC serving as the Interconnection Time Monitor failed to initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Procedure.
BAL-004-0	R4.1.	Balancing Authorities that have reliability concerns with the execution of a Time Error Correction shall notify their Reliability Coordinator and request the termination of a Time Error Correction in progress.	N/A	N/A	N/A	The Balancing Authority with reliability concerns failed to notify the Reliability Coordinator and request the termination of a Time Error Correction in progress.
BAL-005-0.1b	R1.	All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	N/A
BAL-005-0.1b	R1.1.	Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	The Generator Operator with generation facilities operating in an Interconnection failed to ensure that those generation facilities were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.1b	R1.2.	Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are	N/A	N/A	N/A	The Transmission Operator with transmission facilities operating in an Interconnection

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		included within the metered boundaries of a Balancing Authority Area.				failed to ensure that those transmission facilities were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.1b	R1.3.	Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	The Load-Serving Entity with load operating in an Interconnection failed to ensure that those loads were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.1b	R2.	Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.	N/A	N/A	N/A	The Balancing Authority failed to maintain Regulating Reserve that can be controlled by AGC to meet Control Performance Standard.
BAL-005-0.1b	R3.	A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.	N/A	N/A	N/A	The Balancing Authority providing Regulation Service failed to ensure adequate metering, communications, and control equipment was provided.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-005-0.1b	R4.	A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority providing Regulation Service failed to notify the Host Balancing Authority for whom it is controlling if it was unable to provide the service, as well as any Intermediate Balancing Authorities.
BAL-005-0.1b	R5.	A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.	N/A	N/A	N/A	The Balancing Authority receiving Regulation Service failed to ensure that back-up plans were in place to provide replacement Regulation Service.
BAL-005-0.1b	R6.	The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes	The Balancing Authority failed to notify the Reliability Coordinator within 30 minutes of its inability to calculate ACE.	The Balancing Authority failed to calculate ACE as specified in the requirement.	N/A	The Balancing Authority failed to notify the Reliability Coordinator within 30 minutes of its inability to calculate ACE and failed to use the ACE calculation specified in the requirement in its attempt to calculate ACE.

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		it shall notify its Reliability Coordinator.				
BAL-005-0.1b	R7.	The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.	N/A	N/A	N/A	The Balancing Authority failed to operate AGC continuously when there were no adverse impacts OR if their AGC was inoperative the Balancing Authority failed to use manual control to adjust generation to maintain the Net Scheduled Interchange.
BAL-005-0.1b	R8.	The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.	N/A	N/A	N/A	The Balancing Authority failed to ensure that data acquisition for and calculation of ACE occurred at least every six seconds.
BAL-005-0.1b	R8.1.	Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.	N/A	N/A		The Balancing Authority failed to provide redundant and independent frequency metering equipment that automatically activated upon detection of failure, such that the minimum availability was less

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						than 99.95%.
BAL-005-0.1b	R9.	The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.	N/A	N/A	N/A	The Balancing Authority failed to include all Interchanged Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.
BAL-005-0.1b	R9.1.	Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.	N/A	N/A	N/A	The Balancing Authority with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection chose to omit the Interchange Schedule related to the HVDC link from the ACE equation. but failed to model it as internal generation or load.
BAL-005-0.1b	R10.	The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.	N/A	N/A	N/A	The Balancing Authority failed to include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-005-0.1b	R11.	Balancing Authorities shall include the effect of Ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.	N/A	N/A	N/A	The Balancing Authority failed to include the effect of Ramp rates in the Scheduled Interchange values to calculate ACE.
BAL-005-0.1b	R12.	Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.	N/A	N/A	N/A	The Balancing Authority failed to include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.
BAL-005-0.1b	R12.1.	Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.	N/A	N/A	N/A	The Balancing Authority failed to ensure Tie Line MW metering was telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. OR The Balancing Authority failed to ensure that megawatt-hour data is telemetered or reported at the end of each hour.
BAL-005-	R12.2.	Balancing Authorities shall	N/A	N/A	N/A	The Balancing

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
0.1b		ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.				Authority failed to ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service were filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.
BAL-005-0.1b	R12.3.	Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.	N/A	N/A	N/A	The Balancing Authority failed to install common metering equipment where Dynamic Schedules or Pseudo-Ties were implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.
BAL-005-0.1b	R13.	Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the	N/A	N/A	N/A	The Balancing Authority failed to perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.				accuracy of its control equipment OR the Balancing Authority failed to adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.
BAL-005-0.1b	R14.	The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.	N/A	N/A	N/A	The Balancing Authority failed to provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance.
BAL-005-0.1b	R15.	The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing	N/A	N/A	The Balancing Authority failed to periodically test backup power supplies at the	The Balancing Authority failed to provide adequate and reliable backup power supplies to

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authority's control center and other critical locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.			Balancing Authority's control center and other critical locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.	ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.
BAL-005-0.1b	R16.	The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.	The Balancing Authority failed to collect coincident data to the greatest practical extent.	N/A	The Balancing Authority failed to flag missing or bad data for operator display and archival purposes.	The Balancing Authority failed to sample data at least at the same periodicity with which ACE is calculated.
BAL-005-0.1b	R17.	Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below: <i>See Standard for Values</i>	N/A	N/A	N/A	The Balancing Authority failed to at least annually check and calibrate its time error and frequency devices against a common reference.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-006-1.1	R1.	Each Balancing Authority shall calculate and record hourly Inadvertent Interchange.	N/A	N/A	N/A	Each Balancing Authority failed to calculate and record hourly Inadvertent Interchange.
BAL-006-1.1	R2.	Each Balancing Authority shall include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. The Balancing Authority shall take into account interchange served by jointly owned generators.	N/A	N/A	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. OR Failed to take into account interchange served by jointly owned generators.	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. AND Failed to take into account interchange served by jointly owned generators.
BAL-006-1.1	R3.	Each Balancing Authority shall ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority failed to ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-006-1.1	R4.	Adjacent Balancing Authority Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign. Each Balancing Authority shall compute its Inadvertent Interchange based on the following:	The Balancing Authority failed to record Actual Net Interchange values that are equal but opposite in sign to its Adjacent Balancing Authorities.	The Balancing Authority failed to compute Inadvertent Interchange.	The Balancing Authority failed to operate to a common Net Interchange Schedule that is equal but opposite to its Adjacent Balancing Authorities.	N/A
BAL-006-1.1	R4.1.	Each Balancing Authority, by the end of the next business day, shall agree with its Adjacent Balancing Authorities to:	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net Interchanged Schedule. AND The hourly integrated megawatt-hour values of Net Actual Interchange.
BAL-006-1.1	R4.1.1.	The hourly values of Net Interchange Schedule.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Interchanged Schedule.
BAL-006-1.1	R4.1.2.	The hourly integrated megawatt-hour values of Net Actual Interchange.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly integrated megawatt-hour values of Net Actual Interchange.
BAL-006-1.1	R4.2.	Each Balancing Authority shall use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.	N/A	N/A	N/A	The Balancing Authority failed to use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.
BAL-006-1.1	R4.3.	A Balancing Authority shall make after-the-fact corrections to the agreed-to daily and monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). Changes or corrections based on non-reliability considerations shall not be	N/A	N/A	N/A	The Balancing Authority failed to make after-the-fact corrections to the agreed-to daily and monthly accounting data to reflect actual operating conditions or changes or corrections based on non-reliability

**Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reflected in the Balancing Authority's Inadvertent Interchange. After-the-fact corrections to scheduled or actual values will not be accepted without agreement of the Adjacent Balancing Authority(ies).				considerations were reflected in the Balancing Authority's Inadvertent Interchange.
BAL-006-1.1	R5.	Adjacent Balancing Authorities that cannot mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month shall, for the purposes of dispute resolution, submit a report to their respective Regional Reliability Organization Survey Contact. The report shall describe the nature and the cause of the dispute as well as a process for correcting the discrepancy.	Adjacent Balancing Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities, submitted a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute but failed to provide a process for correcting the discrepancy.	Adjacent Balancing Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month, failed to submit a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute as well as a process for correcting the discrepancy.	N/A	N/A

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-001-1	R1.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	N/A	N/A	The responsible entity has procedures for the recognition of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection but does not have a procedure for making their operating personnel aware of said events.	The responsible entity failed to have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.
CIP-001-1	R2.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	N/A	N/A	The responsible entity has demonstrated the existence of a procedure to communicate information concerning sabotage events, but not all of the appropriate parties in the interconnection are identified.	The responsible entity failed to have a procedure for communicating information concerning sabotage events.
CIP-001-1	R3.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and	N/A	The responsible entity has demonstrated the existence of a	The responsible entity has demonstrated the existence of a	The responsible entity failed to have a response guideline for reporting

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.		response guideline for reporting disturbances due to sabotage events, but the guideline did not list all of the appropriate personnel to contact.	response guideline for reporting disturbances due to sabotage events, including all of the appropriate personnel to contact, but the guideline was not available to its operating personnel.	disturbances due to sabotage events.
CIP-001-1	R4.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	N/A	N/A	The responsible entity has established communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, but has not developed a reporting procedure.	The responsible entity failed to establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, nor developed a reporting procedure.
CIP-002-2	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-2	R2.	<p>may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)</p> <p>Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.</p>	N/A	N/A	N/A	<p>identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)</p> <p>The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.</p>
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
CIP-003-2	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific	N/A	N/A	The identification of a senior manager's delegate does not include at least one of	A senior manager's delegate is not identified by name, title, and date of

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.			the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.
CIP-003-2	R2.4.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-2	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-004-2	R1.	<p>Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:</p> <ul style="list-style-type: none"> • Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications (e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, 	<p>The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.</p>	<p>The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.</p>	<p>The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.</p>	<p>The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.</p>

Complete Violation Severity Level Matrix (CIP) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		etc.).				
CIP-004-2	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, implement, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-2	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-2	R3.	Personnel Risk Assessment — The Responsible Entity shall	N/A	The Responsible Entity has a	The Responsible Entity has a	The Responsible Entity does not have

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.		personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
CIP-005-2	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3, Standard CIP-007-2 Requirements R1 and R3 through R9;; Standard CIP-008-2; and Standard CIP-009-2.	protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9;; Standard CIP-008-2; and Standard CIP-009-2.	protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	more of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3;; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3;; Standard CIP-007-2 Requirements R1 and R3 through R9;; Standard CIP-008-2; and Standard CIP-009-2.
CIP-005-2	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum,	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).	The Responsible Entity did not document, implement, and maintain a physical security plan.

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the following:			OR The Responsible Entity created and implemented but did not maintain a physical security plan.	
CIP-006-2	R1.1	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to the Critical such Cyber Assets within the Electronic Security Perimeter.

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-2	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	The Responsible Entity's physical security plan addresses a process for updating the physical security plan within-thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within thirty calendar days of the completion of a physical security system redesign or reconfiguration.
CIP-006-2	R1.8.	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						physical security plan is reviewed at least annually.
CIP-006-2	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						was provided without four (4) or more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
CIP-006-2	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
CIP-006-2	R4.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s)	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s)	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s)

Complete Violation Severity Level Matrix (CIP) Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>shall implement one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber 		<p>twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, 	<p>twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, 	<p>twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric,

Complete Violation Severity Level Matrix (CIP) Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Assets.		keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-2	R5.	<p>Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:</p> <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible 	N/A	<p>The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:</p> <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: 	<p>The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:</p> <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: 	<p>The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:</p> <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points:

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>for response.</p> <ul style="list-style-type: none"> Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. 		Monitoring of physical access points by authorized personnel as specified in Requirement R4.	Monitoring of physical access points by authorized personnel as specified in Requirement R4.	<p>Monitoring of physical access points by authorized personnel as specified in Requirement R4.</p> <p>OR</p> <p>An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-2.</p>
CIP-006-2	R6.	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible 	<p>The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity's 	<p>The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity's selected access 	<p>The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity's 	<p>The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> Computerized Logging: Electronic logs produced by the Responsible Entity's

Complete Violation Severity Level Matrix (CIP) Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>Entity's selected access control and monitoring method.</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. 	<p>selected access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. 	<p>control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. 	<p>selected access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. 	<p>selected access control and monitoring method,</p> <ul style="list-style-type: none"> • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
CIP-006-2	R7.	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in	The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar	The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar	The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar	The Responsible Entity retained physical access logs for less than 45 calendar days.

Complete Violation Severity Level Matrix (CIP) Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		accordance with the requirements of Standard CIP-008-2.	days.	days.	days.	
CIP-006-2	R8.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.
CIP-007-2	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
CIP-007-2	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented	The Responsible Entity established (implemented) and documented, either	The Responsible Entity established (implemented) but did not document,	The Responsible Entity documented but did not establish (implement), either	The Responsible Entity did not establish (implement) nor

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	document , either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-2	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-2	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.
CIP-007-2	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not maintain records as specified in R7.3.	redeployment as specified in R7.2.	disposal as specified in R7.1.	Standard CIP-005-2.
CIP-007-2	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.
CIP-008-2	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.

**Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-009-2	R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 30 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
COM-001-1.1	R1.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information:	The responsible entity's telecommunications is not redundant or diversely routed as applicable by other operating entities for the exchange of interconnection or operating data.	The responsible entity's telecommunications is not redundant or diversely routed as applicable and has failed to establish telecommunications internally for the exchange of interconnection or operating data needed to maintain BES reliability.	The responsible entity's telecommunications is not redundant or diversely routed as applicable and has failed to establish telecommunications internally and with other Reliability Coordinators, Transmission Operators, or Balancing Authorities for the exchange of interconnection or operating data needed to maintain BES reliability.	The responsible entity's telecommunications is not redundant or diversely routed as applicable and has failed to establish telecommunications internally and with both other and its Reliability Coordinators, Transmission Operators, or Balancing Authorities for the exchange of interconnection or operating data needed to maintain BES reliability.
COM-001-1.1	R1.1.	Internally.	N/A	N/A	N/A	The responsible entity has failed to establish telecommunications internally for the exchange of interconnection or operating data needed to maintain BES reliability.
COM-001-1.1	R1.2.	Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.	N/A	N/A	N/A	The responsible entity has failed to establish telecommunications

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						with its Reliability Coordinator, Transmission Operators, or Balancing Authorities for the exchange of interconnection or operating data needed to maintain BES reliability.
COM-001-1.1	R1.3.	With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.	N/A	N/A	NA	The responsible entity has failed to establish telecommunications with other Reliability Coordinators, Transmission Operators, or Balancing Authorities for the exchange of interconnection or operating data needed to maintain BES reliability.
COM-001-1.1	R1.4.	Where applicable, these facilities shall be redundant and diversely routed.	N/A	N/A	N/A	The responsible entity's telecommunications is not redundant or diversely routed where applicable for the exchange of interconnection or operating data.
COM-001-1.1	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall	N/A	The responsible entity has failed to manage, alarm, and	The responsible entity has failed to manage, alarm, and	The responsible entity has failed to manage, alarm, and

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.		test or actively monitor its emergency telecommunications facilities.	test or actively monitor its primary telecommunications facilities.	test or actively monitor its primary and emergency telecommunications facilities.
COM-001-1.1	R3.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate telecommunications among their respective areas. This coordination shall include the ability to investigate and recommend solutions to telecommunications problems within the area and with other areas.	N/A	N/A	The responsible entity failed to assist in the investigation and recommending of solutions to telecommunications problems within the area and with other areas.	The responsible entity failed to provide a means to coordinate telecommunications among their respective areas including assisting in the investigation and recommending of solutions to telecommunications problems within the area and with other areas.
COM-001-1.1	R4.	Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing	N/A	N/A	N/A	If using a language other than English, the responsible entity failed to provide documentation of agreement to use a language other than English for all communications between and among operating personnel responsible for the real-time generation

Complete Violation Severity Level Matrix (COM) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authorities may use an alternate language for internal operations.				control and operation of the interconnected Bulk Electric System.
COM-001-1.1	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.	N/A	N/A	N/A	The responsible entity did not have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.
COM-001-1.1	R6.	Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."	The NERCNet User Organization failed to adhere to less than 25% of the requirements listed in COM-001-0, Attachment 1, "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to 25% or more but less than 50% of the requirements listed in COM-001-0, Attachment 1, "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to 50% or more but less than 75% of the requirements listed in COM-001-0, Attachment 1, "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to 75% or more of the requirements listed in COM-001-0, Attachment 1, "NERCNet Security Policy".
COM-002-2	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. Such communications shall be staffed and available for addressing a real-time emergency condition.	N/A	The responsible entity did not have data links with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators.	The responsible entity did not staff the communications (voice and data links) on a 24 hour basis.	The responsible entity failed to have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators.
COM-002-2	R1.1.	Each Balancing Authority and	N/A	N/A	The responsible	The responsible

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Operator shall notify its Reliability Coordinator, and all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.			entity failed to notify all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.	entity failed to notify its Reliability Coordinator, and all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.
COM-002-2	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall issue directives in a clear, concise, and definitive manner; shall ensure the recipient of the directive repeats the information back correctly; and shall acknowledge the response as correct or repeat the original statement to resolve any misunderstandings.	N/A	The responsible entity provided a clear directive in a clear, concise and definitive manner and required the recipient to repeat the directive, but did not acknowledge the recipient was correct in the repeated directive.	The responsible entity provided a clear directive in a clear, concise and definitive manner, but did not require the recipient to repeat the directive.	The responsible entity failed to provide a clear directive in a clear, concise and definitive manner when required.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-001-0	R1.	Balancing Authorities shall have operating agreements with adjacent Balancing Authorities that shall, at a minimum, contain provisions for emergency assistance, including provisions to obtain emergency assistance from remote Balancing Authorities.	The Balancing Authority failed to demonstrate the existence of the necessary operating agreements for less than 25% of the adjacent BAs. Or less than 25% of those agreements do not contain provisions for emergency assistance.	The Balancing Authority failed to demonstrate the existence of the necessary operating agreements for 25% to 50% of the adjacent BAs. Or 25 to 50% of those agreements do not contain provisions for emergency assistance.	The Balancing Authority failed to demonstrate the existence of the necessary operating agreements for 50% to 75% of the adjacent BAs. Or 50% to 75% of those agreements do not contain provisions for emergency assistance.	The Balancing Authority failed to demonstrate the existence of the necessary operating agreements for 75% or more of the adjacent BAs. Or more than 75% of those agreements do not contain provisions for emergency assistance.
EOP-001-0	R2.	The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. The plan shall include the details on how the Transmission Operator will implement load reduction in sufficient amount and time to mitigate the IROL violation before system separation or collapse would occur. The load reduction plan must be capable of being implemented within 30 minutes.	The Transmission Operator has demonstrated the existence of the emergency load reduction plan but the plan will take longer than 30 minutes.	N/A	The Transmission Operator fails to include details on how load reduction is to be implemented in sufficient amount and time to mitigate IROL violation.	The Transmission Operator failed to demonstrate the existence of emergency load reduction plans for all identified IROLs.
EOP-001-0	R3.	Each Transmission Operator and Balancing Authority shall:	The Transmission Operator or Balancing Authority failed to comply with one (1) of the sub-components.	The Transmission Operator or Balancing Authority failed to comply with two (2) of the sub-components.	The Transmission Operator or Balancing Authority has failed to comply with three (3) of the sub-components.	The Transmission Operator or Balancing Authority has failed to comply with four (4) of the sub-components.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-001-0	R3.1.	Develop, maintain, and implement a set of plans to mitigate operating emergencies for insufficient generating capacity.	The Transmission Operator or Balancing Authority's emergency plans to mitigate insufficient generating capacity are missing minor details or minor program/procedural elements.	The Transmission Operator or Balancing Authority's has demonstrated the existence of emergency plans to mitigate insufficient generating capacity emergency plans but the plans are not maintained.	The Transmission Operator or Balancing Authority's emergency plans to mitigate insufficient generating capacity emergency plans are not maintained nor implemented.	The Transmission Operator or Balancing Authority has failed to develop emergency mitigation plans for insufficient generating capacity.
EOP-001-0	R3.2.	Develop, maintain, and implement a set of plans to mitigate operating emergencies on the transmission system.	The Transmission Operator or Balancing Authority's plans to mitigate transmission system emergencies are missing minor details or minor program/procedural elements.	The Transmission Operator or Balancing Authority's has demonstrated the existence of transmission system emergency plans but are not maintained.	The Transmission Operator or Balancing Authority's transmission system emergency plans are not maintained nor implemented.	The Transmission Operator or Balancing Authority has failed to develop, maintain, and implement operating emergency mitigation plans for emergencies on the transmission system.
EOP-001-0	R3.3.	Develop, maintain, and implement a set of plans for load shedding.	The Transmission Operator or Balancing Authority's load shedding plans are missing minor details or minor program/procedural elements.	The Transmission Operator or Balancing Authority's has demonstrated the existence of load shedding plans but are not maintained.	The Transmission Operator or Balancing Authority's load shedding plans are partially compliant with the requirement but are not maintained nor implemented.	The Transmission Operator or Balancing Authority has failed to develop, maintain, and implement load shedding plans.
EOP-001-0	R3.4.	Develop, maintain, and implement a set of plans for	The Transmission Operator or	The Transmission Operator or	The Transmission Operator or	The Transmission Operator or

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		system restoration.	Balancing Authority's system restoration plans are missing minor details or minor program/procedural elements.	Balancing Authority's system restoration plans are partially compliant with the requirement but are not maintained.	Balancing Authority's restoration plans are not maintained nor implemented.	Balancing Authority has failed to develop, maintain, and implement operating emergency mitigation plans for system restoration.
EOP-001-0	R4.	Each Transmission Operator and Balancing Authority shall have emergency plans that will enable it to mitigate operating emergencies. At a minimum, Transmission Operator and Balancing Authority emergency plans shall include:	The Transmission Operator or Balancing Authority failed to comply with one (1) of the sub-components.	The Transmission Operator or Balancing Authority failed to comply with two (2) of the sub-components.	The Transmission Operator or Balancing Authority has failed to comply with three (3) of the sub-components.	The Transmission Operator or Balancing Authority has failed to comply with all four (4) of the sub-components.
EOP-001-0	R4.1.	Communications protocols to be used during emergencies.	The Transmission Operator or Balancing Authority's communication protocols included in the emergency plan are missing minor program/procedural elements.	N/A	N/A	The Transmission Operator or Balancing Authority has failed to include communication protocols in its emergency plans to mitigate operating emergencies.
EOP-001-0	R4.2.	A list of controlling actions to resolve the emergency. Load reduction, in sufficient quantity to resolve the emergency within NERC-established timelines, shall be one of the controlling actions.	The Transmission Operator or Balancing Authority's list of controlling actions has resulted in meeting the intent of the requirement but is missing minor	N/A	The Transmission Operator or Balancing Authority provided a list of controlling actions; however the actions fail to resolve the emergency within NERC-established	The Transmission Operator or Balancing Authority has failed to provide a list of controlling actions to resolve the emergency.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			program/procedural elements.		timelines.	
EOP-001-0	R4.3.	The tasks to be coordinated with and among adjacent Transmission Operators and Balancing Authorities.	The Transmission Operator or Balancing Authority has demonstrated coordination with Transmission Operators and Balancing Authorities but is missing minor program/procedural elements.	N/A	N/A	The Transmission Operator or Balancing Authority has failed to demonstrate the tasks to be coordinated with adjacent Transmission Operator and Balancing Authorities as directed by the requirement.
EOP-001-0	R4.4.	Staffing levels for the emergency.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority's emergency plan does not include staffing levels for the emergency
EOP-001-0	R5.	Each Transmission Operator and Balancing Authority shall include the applicable elements in Attachment 1-EOP-001-0 when developing an emergency plan.	The Transmission Operator and Balancing Authority emergency plan has complied with 90% or more of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with 70% to 90% of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with between 50% to 70% of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with 50% or less of the number of sub-components
EOP-001-0	R6.	The Transmission Operator and Balancing Authority shall annually review and update each emergency plan. The	The Transmission Operator and Balancing Authority is missing minor	The Transmission Operator and Balancing Authority has failed to	The Transmission Operator and Balancing Authority has failed to	The Transmission Operator and Balancing Authority has failed to

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Operator and Balancing Authority shall provide a copy of its updated emergency plans to its Reliability Coordinator and to neighboring Transmission Operators and Balancing Authorities.	program/procedural elements.	annually review one of its emergency plans	annually review 2 of its emergency plans or communicate with 1 of its neighboring Balancing Authorities.	annually review and/or communicate any emergency plans with its Reliability Coordinator, neighboring Transmission Operators or Balancing Authorities.
EOP-001-0	R7.	The Transmission Operator and Balancing Authority shall coordinate its emergency plans with other Transmission Operators and Balancing Authorities as appropriate. This coordination includes the following steps, as applicable:	The Transmission Operator and/or the Balancing Authority failed to comply with one (1) of the sub-components.	The Transmission Operator and/or the Balancing Authority failed to comply with two (2) of the sub-components.	The Transmission Operator and/or the Balancing Authority has failed to comply with three (3) of the sub-components.	The Transmission Operator and/or the Balancing Authority has failed to comply with four (4) or more of the sub-components.
EOP-001-0	R7.1.	The Transmission Operator and Balancing Authority shall establish and maintain reliable communications between interconnected systems.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to establish and maintain reliable communication between interconnected systems.
EOP-001-0	R7.2.	The Transmission Operator and Balancing Authority shall arrange new interchange agreements to provide for emergency capacity or energy transfers if existing agreements cannot be used.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to arrange new interchange agreements to

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						provide for emergency capacity or energy transfers with required entities when existing agreements could not be used.
EOP-001-0	R7.3.	The Transmission Operator and Balancing Authority shall coordinate transmission and generator maintenance schedules to maximize capacity or conserve the fuel in short supply. (This includes water for hydro generators.)	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to coordinate transmission and generator maintenance schedules to maximize capacity or conserve fuel in short supply.
EOP-001-0	R7.4.	The Transmission Operator and Balancing Authority shall arrange deliveries of electrical energy or fuel from remote systems through normal operating channels.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to arrange for deliveries of electrical energy or fuel from remote systems through normal operating channels.
EOP-002-2.1	R1.	Each Balancing Authority and Reliability Coordinator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its respective area and shall exercise	N/A	N/A	N/A	The Balancing Authority or Reliability Coordinator does not have responsibility and clear decision-

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		specific authority to alleviate capacity and energy emergencies.				making authority to take whatever actions are needed to ensure the reliability of its respective area OR The Balancing Authority or Reliability Coordinator did not exercise its authority to alleviate capacity and energy emergencies.
EOP-002-2.1	R2.	Each Balancing Authority shall implement its capacity and energy emergency plan, when required and as appropriate, to reduce risks to the interconnected system.	N/A	N/A	N/A	The Balancing Authority did not implement its capacity and energy emergency plan, when required and as appropriate, to reduce risks to the interconnected system.
EOP-002-2.1	R3.	A Balancing Authority that is experiencing an operating capacity or energy emergency shall communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.	N/A	N/A	The Balancing Authority communicated its current and future system conditions to its Reliability Coordinator but did not communicate to one or more of its neighboring Balancing Authorities.	The Balancing Authority has failed to communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-002-2.1	R4.	A Balancing Authority anticipating an operating capacity or energy emergency shall perform all actions necessary including bringing on all available generation, postponing equipment maintenance, scheduling interchange purchases in advance, and being prepared to reduce firm load.	N/A	N/A	N/A	The Balancing Authority has failed to perform the necessary actions as required and stated in the requirement.
EOP-002-2.1	R5.	A deficient Balancing Authority shall only use the assistance provided by the Interconnection's frequency bias for the time needed to implement corrective actions. The Balancing Authority shall not unilaterally adjust generation in an attempt to return Interconnection frequency to normal beyond that supplied through frequency bias action and Interchange Schedule changes. Such unilateral adjustment may overload transmission facilities.	N/A	N/A	The Balancing Authority used the assistance provided by the Interconnection's frequency bias for more time than needed to implement corrective actions.	The Balancing Authority used the assistance provided by the Interconnection's frequency bias for more time than needed to implement corrective actions and unilaterally adjust generation in an attempt to return Interconnection frequency to normal beyond that supplied through frequency bias action and Interchange Schedule changes.
EOP-002-2.1	R6.	If the Balancing Authority cannot comply with the Control Performance and Disturbance Control Standards, then it shall immediately implement remedies	The Balancing Authority failed to comply with one of the sub-components.	The Balancing Authority failed to comply with 2 of the sub-components.	The Balancing Authority failed to comply with 3 of the sub-components.	The Balancing Authority failed to comply with more than 3 of the sub-components.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to do so. These remedies include, but are not limited to:				
EOP-002-2.1	R6.1.	Loading all available generating capacity.	N/A	N/A	N/A	The Balancing Authority did not use all available generating capacity.
EOP-002-2.1	R6.2.	Deploying all available operating reserve	N/A	N/A	N/A	The Balancing Authority did not deploy all of its available operating reserve.
EOP-002-2.1	R6.3.	Interrupting interruptible load and exports.	N/A	N/A	N/A	The Balancing Authority did not interrupt interruptible load and exports.
EOP-002-2.1	R6.4.	Requesting emergency assistance from other Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority did not request emergency assistance from other Balancing Authorities.
EOP-002-2.1	R6.5.	Declaring an Energy Emergency through its Reliability Coordinator; and	N/A	N/A	N/A	The Balancing Authority did not declare an Energy Emergency through its Reliability Coordinator.
EOP-002-2.1	R6.6.	Reducing load, through procedures such as public appeals, voltage reductions, curtailing interruptible loads and firm loads.	N/A	N/A	N/A	The Balancing Authority did not implement one or more of the procedures stated in the requirement.
EOP-002-2.1	R7.	Once the Balancing Authority has exhausted the steps listed in	N/A	N/A	The Balancing Authority has met	The Balancing Authority has not

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirement 6, or if these steps cannot be completed in sufficient time to resolve the emergency condition, the Balancing Authority shall:			only one of the two requirements	met either of the two requirements
EOP-002-2.1	R7.1.	Manually shed firm load without delay to return its ACE to zero; and	N/A	N/A	N/A	The Balancing Authority did not manually shed firm load without delay to return its ACE to zero.
EOP-002-2.1	R7.2.	Request the Reliability Coordinator to declare an Energy Emergency Alert in accordance with Attachment 1-EOP-002-0 "Energy Emergency Alert Levels."	The Balancing Authority's implementation of an Energy Emergency Alert has missed minor program/procedural elements in Attachment 1-EOP-002-0.	N/A	N/A	The Balancing Authority has failed to meet one or more of the requirements of Attachment 1-EOP-002-0.
EOP-002-2.1	R8.	A Reliability Coordinator that has any Balancing Authority within its Reliability Coordinator area experiencing a potential or actual Energy Emergency shall initiate an Energy Emergency Alert as detailed in Attachment 1-EOP-002-0 "Energy Emergency Alert Levels." The Reliability Coordinator shall act to mitigate the emergency condition, including a request for emergency assistance if required.	The Reliability Coordinator's implementation of an Energy Emergency Alert has missed minor program/procedural elements in Attachment 1-EOP-002-0.	N/A	N/A	The Reliability Coordinator has failed to meet one or more of the requirements of Attachment 1-EOP-002-0.
EOP-002-2.1	R9.	When a Transmission Service Provider expects to elevate the	The Reliability Coordinator failed	The Reliability Coordinator failed	The Reliability Coordinator has	The Reliability Coordinator has

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources) as permitted in its transmission tariff (See Attachment 1-IRO-006-0 "Transmission Loading Relief Procedure" for explanation of Transmission Service Priorities):	to comply with one (1) of the sub-components.	to comply with two (2) of the sub-components.	failed to comply with three (3) of the sub-components.	failed to comply with all four (4) of the sub-components.
EOP-002-2.1	R9.1.	The deficient Load-Serving Entity shall request its Reliability Coordinator to initiate an Energy Emergency Alert in accordance with Attachment 1-EOP-002-0.	N/A	N/A	N/A	The Load-Serving Entity failed to request its Reliability Coordinator to initiate an Energy Emergency Alert.
EOP-002-2.1	R9.2.	The Reliability Coordinator shall submit the report to NERC for posting on the NERC Website, noting the expected total MW that may have its transmission service priority changed.	N/A	N/A	N/A	The Reliability Coordinator has failed to report to NERC as directed in the requirement.
EOP-002-2.1	R9.3.	The Reliability Coordinator shall use EEA 1 to forecast the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to Priority 7.	N/A	N/A	N/A	The Reliability Coordinator failed to use EEA 1 to forecast the change of the priority of transmission service as directed in the requirement.
EOP-002-	R9.4.	The Reliability Coordinator shall	N/A	N/A	N/A	The Reliability

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
2.1		use EEA 2 to announce the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to Priority 7.				Coordinator failed to use EEA 2 to announce the change of the priority of transmission service as directed in the requirement.
EOP-003-1	R1.	After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed shed customer load.
EOP-003-1	R2.	Each Transmission Operator and Balancing Authority shall establish plans for automatic load shedding for underfrequency or undervoltage conditions.	N/A	N/A	N/A	The applicable entity did not establish plans for automatic load-shedding, as directed by the requirement.
EOP-003-1	R3.	Each Transmission Operator and Balancing Authority shall coordinate load shedding plans among other interconnected Transmission Operators and Balancing Authorities.	The applicable entity did not coordinate load shedding plans, as directed by the requirement, affecting 5% or less of its required entities.	The applicable entity did not coordinate load shedding plans, as directed by the requirement, affecting between 5-10% of its required entities.	The applicable entity did not coordinate load shedding plans, as directed by the requirement, affecting 10-15%, inclusive, of its required entities.	The applicable entity did not coordinate load shedding plans, as directed by the requirement, affecting greater than 15% of its required entities.
EOP-003-1	R4.	A Transmission Operator or Balancing Authority shall consider one or more of these	N/A	N/A	N/A	The applicable entity did not consider one of the

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		factors in designing an automatic load shedding scheme: frequency, rate of frequency decay, voltage level, rate of voltage decay, or power flow levels.				five required elements, as directed by the requirement.
EOP-003-1	R5.	A Transmission Operator or Balancing Authority shall implement load shedding in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to implement load shedding as directed in the requirement.
EOP-003-1	R6.	After a Transmission Operator or Balancing Authority Area separates from the Interconnection, if there is insufficient generating capacity to restore system frequency following automatic underfrequency load shedding, the Transmission Operator or Balancing Authority shall shed additional load.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority did not shed load.
EOP-003-1	R7.	The Transmission Operator and Balancing Authority shall coordinate automatic load shedding throughout their areas with underfrequency isolation of generating units, tripping of shunt capacitors, and other automatic actions that will occur under abnormal frequency, voltage, or power flow conditions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting 5% or less of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting between 5 -10% of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting 10-15%, inclusive, of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting greater than 15% of its automatic actions.
EOP-003-1	R8.	Each Transmission Operator or Balancing Authority shall have plans for operator-controlled	N/A	The applicable entity did not have plans for operator	The applicable entity did not have the capability to	The applicable entity did not have plans for operator

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be capable of implementing the load shedding in a timeframe adequate for responding to the emergency.		controlled manual load shedding, as directed by the requirement.	implement the load shedding, as directed by the requirement.	controlled manual load shedding, as directed by the requirement nor had the capability to implement the load shedding, as directed by the requirement.
EOP-004-1	R1.	Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	The Regional Reliability Organization has demonstrated the existence of a regional reporting procedure, but the procedure is missing minor details or minor program/procedural elements.	The Regional Reliability Organization Regional reporting procedure have been is missing one element that would make the procedure meet the requirement.	The Regional Reliability Organization Regional has a regional reporting procedure but the procedure is not current.	The Regional Reliability Organization does not have a regional reporting procedure.
EOP-004-1	R2.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	N/A	The responsible entities has failed to analyze 1% to 25% of its disturbances on the BES or was negligent in the timeliness of analyzing the disturbances 1% to 25% of the time.	The responsible entities has failed to analyze 26% to 50% of its disturbances on the BES or was negligent in the timeliness of analyzing the disturbances 26% to 50% of the time.	The responsible entities has failed to analyze more than 50% of its disturbances on the BES or negligent in the timeliness of analyzing the disturbances more than 50% of the time
EOP-004-1	R3.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity	N/A	N/A	N/A	The responsible entities failed to provide a preliminary written

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.				report as directed by the requirement.
EOP-004-1	R3.1.	The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.		The responsible entities submitted the report within 25 to 36 hours of the disturbance or discovery of the disturbance.	The responsible entities submitted the report within 36 to 48 hours of the disturbance or discovery of the disturbance.	The responsible entities submitted the report more than 48 hours after the disturbance or discovery of the disturbance.
EOP-004-1	R3.2.	Applicable reporting forms are provided in Attachments 022-1 and 022-2.	N/A	N/A	N/A	N/A
EOP-004-1	R3.3.	Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission	The responsible entity provided its Reliability Coordinator and NERC with periodic, verbal updates about a disturbance, but the updates did not include all information that was	N/A	N/A	The responsible entity did not provide its Reliability Coordinator and NERC with verbal updates about a disturbance as specified in R3.3.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	available at the time.			
EOP-004-1	R3.4.	If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event.	The responsible entities final report is missing minor details or minor program/procedural elements.	The responsible entities final report was 30 days late or was missing one of the elements specified in the requirement.	The responsible entities final report was more than 30 days late or was missing two of the elements specified in the requirement.	The responsible entities final report was not submitted or was missing more than two of the elements specified in the requirement.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The report shall be subject to Regional Reliability Organization approval.				
EOP-004-1	R4.	When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	N/A	N/A	N/A	The RRO did not make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.
EOP-004-1	R5.	The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and	The Regional Reliability Organization reviewed all final report recommendations less than twice a year.	The Regional Reliability Organization reviewed 75% or more final report recommendations twice a year.	The Regional Reliability Organization has not reported on any recommendation has not been acted on within two years to the NERC Planning and Operating Committees.	The Regional Reliability Organization has not reviewed the final report recommendations or did not notify the NERC Planning and Operating Committees.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.				
EOP-005-1	R1.	Each Transmission Operator shall have a restoration plan to reestablish its electric system in a stable and orderly manner in the event of a partial or total shutdown of its system, including necessary operating instructions and procedures to cover emergency conditions, and the loss of vital telecommunications channels. Each Transmission Operator shall include the applicable elements listed in Attachment 1-EOP-005 in developing a restoration plan.	The responsible entity has a restoration plan that includes 75 % or more but less than 100% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes 50% to 75% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes 25% - 50% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes less than 25% of the applicable elements listed in Attachment 1 OR the responsible entity has no restoration plan.
EOP-005-1	R2.	Each Transmission Operator shall review and update its restoration plan at least annually and whenever it makes changes in the power system network, and shall correct deficiencies found during the simulated restoration exercises.	The Transmission Operator failed to review or update its restoration plan when it made changes in the power system network.	The Transmission Operator failed to review and update its restoration plan at least annually.	The Transmission Operator failed to review and update its restoration plan at least annually or whenever it made changes in the power system network, and failed to correct deficiencies found during the simulated restoration exercises.	The Transmission Operator failed to review and update its restoration plan at least annually and whenever it made changes in the power system network, and failed to correct deficiencies found during the simulated restoration exercises.
EOP-005-1	R3.	Each Transmission Operator shall develop restoration plans with a	N/A	N/A	N/A	The Transmission Operator's

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		priority of restoring the integrity of the Interconnection.				restoration plans failed to make restoration of the integrity of the Interconnection a top priority.
EOP-005-1	R4.	Each Transmission Operator shall coordinate its restoration plans with the Generator Owners and Balancing Authorities within its area, its Reliability Coordinator, and neighboring Transmission Operators and Balancing Authorities.	The Transmission Operator failed to coordinate its restoration plans with one of the entities listed in the requirement.	The Transmission Operator failed to coordinate its restoration plans with two of the entities listed in the requirement.	The Transmission Operator failed to coordinate its restoration plans with three of the entities listed in the requirement.	The Transmission Operator failed to coordinate its restoration plans with four or more of the entities listed in the requirement.
EOP-005-1	R5.	Each Transmission Operator and Balancing Authority shall periodically test its telecommunication facilities needed to implement the restoration plan.	N/A	N/A	N/A	The responsible entity failed to periodically test its telecommunication facilities needed to implement the restoration plan.
EOP-005-1	R6.	Each Transmission Operator and Balancing Authority shall train its operating personnel in the implementation of the restoration plan. Such training shall include simulated exercises, if practicable.	The responsible entity only trained less than 100% but greater than or equal to 67 % of its operating personnel in the implementation of the restoration plan.	The responsible entity only trained less than 67 % but greater than or equal to 33 % of its operating personnel in the implementation of the restoration plan.	The responsible entity only trained less than 33 % of its operating personnel in the implementation of the restoration plan.	The responsible entity did not train any of its operating personnel in the implementation of the restoration plan.
EOP-005-1	R7.	Each Transmission Operator and Balancing Authority shall verify the restoration procedure by actual testing or by simulation.	The responsible entity verified 76% to 99% of the restoration procedure by actual testing or by	The responsible entity verified 51% to 75% of the restoration procedure by actual testing or by	The responsible entity verified 26% to 50% of the restoration procedure by actual testing or by	The responsible entity verified less than 26% of the restoration procedure by actual testing or by

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			simulation.	simulation.	simulation.	simulation.
EOP-005-1	R8.	Each Transmission Operator shall verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan requirements for the Transmission Operator's area.	N/A	N/A	N/A	The Transmission Operator failed to verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan requirements for the Transmission Operator's area.
EOP-005-1	R9.	The Transmission Operator shall document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started and shall provide this documentation for review by the Regional Reliability Organization upon request. Such documentation may include Cranking Path diagrams.	N/A	N/A	N/A	The Transmission Operator shall document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started and shall provide this documentation for review by the Regional Reliability Organization upon request.
EOP-005-1	R10.	The Transmission Operator shall demonstrate, through simulation	The Transmission Operator only	The Transmission Operator only	The Transmission Operator only	The Transmission Operator did not

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		or testing, that the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	demonstrated, through simulation or testing, that between 67 and 99% of the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	demonstrated, through simulation or testing, that between 33 and 66% of the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	demonstrated, through simulation or testing, that less than 33% of the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	demonstrate, through simulation or testing, that any of the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.
EOP-005-1	R10.1.	The Transmission Operator shall perform this simulation or testing at least once every five years.	N/A	N/A	N/A	The Transmission Operator failed to perform the required simulation or testing at least once every five years.
EOP-005-1	R11.	Following a disturbance in which one or more areas of the Bulk Electric System become isolated or blacked out, the affected Transmission Operators and Balancing Authorities shall begin immediately to return the Bulk Electric System to normal.	The responsible entity failed to comply with less than 25% of the number of sub-components.	The responsible entity failed to comply with 25% or more and less than 50% of the number of sub-components.	The responsible entity failed to comply with 50% or more and less than 75% of the number of sub-components.	The responsible entity failed to comply with more than 75% of the number of sub-components.
EOP-005-1	R11.1.	The affected Transmission Operators and Balancing Authorities shall work in conjunction with their Reliability Coordinator(s) to determine the extent and condition of the isolated area(s).	N/A	N/A	N/A	The responsible entity failed to work in conjunction with their Reliability Coordinator to determine the extent and condition of the isolated area(s)
EOP-005-1	R11.2.	The affected Transmission	N/A	N/A	N/A	The affected

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators and Balancing Authorities shall take the necessary actions to restore Bulk Electric System frequency to normal, including adjusting generation, placing additional generators on line, or load shedding.				Transmission Operators and Balancing Authorities failed to take the necessary actions to restore Bulk Electric System frequency to normal.
EOP-005-1	R11.3.	The affected Balancing Authorities, working with their Reliability Coordinator(s), shall immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments as needed to facilitate the restoration. The affected Balancing Authorities shall make all attempts to maintain the adjusted Interchange Schedules, whether generation control is manual or automatic.	N/A	N/A	The responsible entity failed to make all attempts to maintain adjusted Interchange Schedules as required in R11.3	The responsible entity failed to immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments to facilitate the restoration as required in R11.3.
EOP-005-1	R11.4.	The affected Transmission Operators shall give high priority to restoration of off-site power to nuclear stations.	N/A	N/A	N/A	The affected Transmission Operators failed to give high priority to restoration of off-site power to nuclear stations.
EOP-005-1	R11.5.	The affected Transmission Operators may resynchronize the isolated area(s) with the surrounding area(s) when the	The responsible entity failed to include one of the subrequirements.	The responsible entity failed to include two of the subrequirements.	The responsible entity failed to include three of the subrequirements.	The responsible entity failed to include four of the subrequirements.

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		following conditions are met:				
EOP-005-1	R11.5.1.	Voltage, frequency, and phase angle permit.	N/A	N/A	N/A	The responsible entity failed to meet this requirement before resynchronizing isolated areas.
EOP-005-1	R11.5.2.	The size of the area being reconnected and the capacity of the transmission lines effecting the reconnection and the number of synchronizing points across the system are considered.	N/A	N/A	N/A	The responsible entity failed to meet this requirement before resynchronizing isolated areas.
EOP-005-1	R11.5.3.	Reliability Coordinator(s) and adjacent areas are notified and Reliability Coordinator approval is given.	N/A	N/A	N/A	The responsible entity failed to meet this requirement before resynchronizing isolated areas.
EOP-005-1	R11.5.4.	Load is shed in neighboring areas, if required, to permit successful interconnected system restoration.	N/A	N/A	N/A	The responsible entity failed to meet this requirement before resynchronizing isolated areas.
EOP-006-1	R1.	Each Reliability Coordinator shall be aware of the restoration plan of each Transmission Operator in its Reliability Coordinator Area in accordance with NERC and regional requirements.	The Reliability Coordinator is aware of more than 75% of its Transmission Operators restoration plans.	The Reliability Coordinator is aware of more than 50% but less than 75% of its Transmission Operators restoration plans.	The Reliability Coordinator is aware of more than 25% but less than 50% of its Transmission Operators restoration plans.	The Reliability Coordinator is not aware of any of its Transmission Operators restoration plans.
EOP-006-1	R2.	The Reliability Coordinator shall monitor restoration progress and coordinate any needed assistance.	N/A	N/A	The Reliability Coordinator failed to monitor	The Reliability Coordinator failed to monitor

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					restoration progress or failed to coordinate assistance.	restoration progress and failed to coordinate assistance.
EOP-006-1	R3.	The Reliability Coordinator shall have a Reliability Coordinator Area restoration plan that provides coordination between individual Transmission Operator restoration plans and that ensures reliability is maintained during system restoration events.	N/A	The Reliability Coordinator's Reliability Coordinator Area restoration plan did not coordinate with one individual Transmission Operator restoration plans.	The Reliability Coordinator's Reliability Coordinator Area restoration plan did not coordinate with more than one individual Transmission Operator restoration plans.	The Reliability Coordinator does not have a Reliability Coordinator Area restoration plan.
EOP-006-1	R4.	The Reliability Coordinator shall serve as the primary contact for disseminating information regarding restoration to neighboring Reliability Coordinators and Transmission Operators or Balancing Authorities not immediately involved in restoration.	The Reliability Coordinator failed to disseminate information regarding restoration to one neighboring Reliability Coordinator or Transmission Operator or Balancing Authority not immediately involved in restoration.	The Reliability Coordinator failed to disseminate information regarding restoration to two neighboring Reliability Coordinators or Transmission Operators or Balancing Authorities not immediately involved in restoration.	The Reliability Coordinator failed to disseminate information regarding restoration to three neighboring Reliability Coordinators or Transmission Operators or Balancing Authorities not immediately involved in restoration.	The Reliability Coordinator failed to disseminate information regarding restoration to four or more neighboring Reliability Coordinators or Transmission Operators or Balancing Authorities not immediately involved in restoration.
EOP-006-1	R5.	Reliability Coordinators shall approve, communicate, and coordinate the re-synchronizing of major system islands or synchronizing points so as not to	N/A	N/A	N/A	The Reliability Coordinators failed to approve, communicate, and coordinate the re-

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cause a Burden on adjacent Transmission Operator, Balancing Authority, or Reliability Coordinator Areas.				synchronizing of major system islands or synchronizing points and caused a Burden on adjacent Transmission Operator, Balancing Authority, or Reliability Coordinator Areas.
EOP-006-1	R6.	The Reliability Coordinator shall take actions to restore normal operations once an operating emergency has been mitigated in accordance with its restoration plan.	N/A	N/A	N/A	The Reliability Coordinator failed to take actions to restore normal operations once an operating emergency has been mitigated in accordance with its restoration plan.
EOP-008-0	R1.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have a plan to continue reliability operations in the event its control center becomes inoperable. The contingency plan must meet the following requirements:	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with one of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with two of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with three or four of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with more than four of the sub-requirements.
EOP-008-0	R1.1.	The contingency plan shall not rely on data or voice communication from the primary control facility to be viable.	The responsible entity's contingency plan relies on data or voice communication from the primary	The responsible entity's contingency plan relies on data or voice communication from the primary	The responsible entity's contingency plan relies on data or voice communication from the primary	The responsible entity's contingency plan relies on data and voice communication from the primary

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			control facility for up to 25% of the functions identified in R1.2 and R1.3.	control facility for 25% to 50% of the functions identified in R1.2 and R1.3.	control facility for 50% to 75% of the functions identified in R1.2 and R1.3.	control facility for more than 75% of the functions identified in R1.2 and R1.3.
EOP-008-0	R1.2.	The plan shall include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.
EOP-008-0	R1.3.	The contingency plan must address monitoring and control of critical transmission facilities, generation control, voltage control, time and frequency control, control of critical substation devices, and logging of significant power system events. The plan shall list the critical facilities.	The responsible entity's contingency plan failed to address one of the elements listed in the requirement.	The responsible entity's contingency plan failed to address two of the elements listed in the requirement.	The responsible entity's contingency plan failed to address three of the elements listed in the requirement.	The responsible entity's contingency plan failed to address four or more of the elements listed in the requirement.
EOP-008-0	R1.4.	The plan shall include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for maintaining basic voice

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						communication capabilities with other areas.
EOP-008-0	R1.5.	The plan shall include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.
EOP-008-0	R1.6.	The plan shall include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.
EOP-008-0	R1.7.	The plan shall be reviewed and updated annually.	The responsible entity's plan was reviewed within 3 months of passing its annual review date.	The responsible entity's plan was reviewed within 6 months of passing its annual review date.	The responsible entity's plan was reviewed within 9 months of passing its annual review date.	The responsible entity's plan was reviewed more than 9 months of passing its annual review date.
EOP-008-0	R1.8.	Interim provisions must be included if it is expected to take more than one hour to implement the contingency plan for loss of primary control facility.	N/A	N/A	N/A	The responsible entity failed to make interim provisions when it is took more than one hour to implement the contingency plan for

**Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						loss of primary control facility.
EOP-009-0	R1.	The Generator Operator of each blackstart generating unit shall test the startup and operation of each system blackstart generating unit identified in the BCP as required in the Regional BCP (Reliability Standard EOP-007-0_R1). Testing records shall include the dates of the tests, the duration of the tests, and an indication of whether the tests met Regional BCP requirements.	The Generator Operator Blackstart unit testing and recording is missing minor program/procedural elements.	Startup and testing of each Blackstart unit was performed, but the testing records are incomplete. The testing records are missing 25% or less of data requested in the requirement'.	The Generator Operator's failed to test 25% or less of the Blackstart units or testing records are incomplete. The testing records are missing between 25% and 50% of data requested in the requirement.	The Generator Operator failed to test more than 25% of its Blackstart units or does not have Blackstart testing records or is missing more than 50% of the required data.
EOP-009-0	R2.	The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.	The Generator Operator has provided the Blackstart testing documentation to its Regional Reliability Organization. However the documentation provided had missing minor program/procedural elements or failed to provide the documentation requested to NERC in 30 days.	N/A	N/A	The Generator Operator did not provide the required Blackstart documentation to its Regional Reliability Organization.

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R1.	The Transmission Owner shall document, maintain, and publish facility connection requirements to ensure compliance with NERC Reliability Standards and applicable Regional Reliability Organization, subregional, Power Pool, and individual Transmission Owner planning criteria and facility connection requirements. The Transmission Owner's facility connection requirements shall address connection requirements for:	Not Applicable.	The Transmission Owner's facility connection requirements failed to address connection requirements for one of the subrequirements.	The Transmission Owner's facility connection requirements failed to address connection requirements for two of the subrequirements.	The Transmission Owner's facility connection requirements failed to address connection requirements for three of the subrequirements.
FAC-001-0	R1.1.	Generation facilities,	The Transmission Owner has Generation facility connection requirements, but they have not been updated to include changes that are currently in effect, but have not been in effect for more than one month.	The Transmission Owner has Generation facility connection requirements, but they have not been updated to include changes that were effective more than one month ago, but not more than six months ago.	The Transmission Owner has Generation facility connection requirements, but they have not been updated to include changes that were effective more than six months ago.	The Transmission Owner does not have Generation facility connection requirements.
FAC-001-0	R1.2.	Transmission facilities, and	The Transmission Owner has Transmission facility connection requirements, but they have not been updated to include changes that are currently in effect,	The Transmission Owner has Transmission facility connection requirements, but they have not been updated to include changes that were effective more than	The Transmission Owner has Transmission facility connection requirements, but they have not been updated to include changes that were effective more than	The Transmission Owner does not have Transmission facility connection requirements.

Complete Violation Severity Level Matrix (FAC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			but have not been in effect for more than one month.	one month ago, but not more than six months ago.	six months ago.	
FAC-001-0	R1.3.	End-user facilities	The Transmission Owner has End-user facility connection requirements, but they have not been updated to include changes that are currently in effect, but have not been in effect for more than one month.	The Transmission Owner has End-user facility connection requirements, but they have not been updated to include changes that were effective more than one month ago, but not more than six months ago.	The Transmission Owner has End-user facility connection requirements, but they have not been updated to include changes that were effective more than six months ago.	The Transmission Owner does not have End-user facility connection requirements.
FAC-001-0	R2.	The Transmission Owner's facility connection requirements shall address, but are not limited to, the following items:	The Transmission Owner's facility connection requirements do not address one to four of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address five to eight of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address nine to twelve of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address thirteen or more of the sub-components. (R2.1.1 to R2.1.16)
FAC-001-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	The Transmission Owner's facility connection requirements do not address one to four of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address five to eight of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address nine to twelve of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address thirteen or more of the sub-components. (R2.1.1 to R2.1.16)
FAC-001-0	R2.1.1.	Procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.2.	Procedures for notification of new or modified facilities to others (those responsible for the reliability of the interconnected transmission systems) as soon as feasible.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.3.	Voltage level and MW and MVAR capacity or demand at point of connection.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.4.	Breaker duty and surge protection.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						systems failed to include this subrequirement.
FAC-001-0	R2.1.5.	System protection and coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.6.	Metering and telecommunications.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.7.	Grounding and safety issues.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R2.1.8.	Insulation and insulation coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.9.	Voltage, Reactive Power, and power factor control.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.10.	Power quality impacts.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.11.	Equipment Ratings.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.12.	Synchronizing of facilities.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.13.	Maintenance coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.14.	Operational issues (abnormal frequency and voltages).	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.15.	Inspection requirements for existing or new facilities.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.16.	Communications and procedures during normal and emergency operating conditions.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R3.	The Transmission Owner shall maintain and update its facility connection requirements as required. The Transmission Owner shall make documentation of these requirements available to the users of the transmission system, the Regional Reliability Organization, and NERC on request (five business days).	The Transmission Owner made the requirements available more than five business days after a request, but not more than ten business days after a request.	The Transmission Owner made the requirements available more than ten business days after a request, but not more than twenty business days after a	The Transmission Owner made the requirements available more than twenty business days after a request, but not more than thirty business days after	The Transmission Owner made the requirements available more than thirty business days after a request.

Complete Violation Severity Level Matrix (FAC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				request.	a request.	
FAC-002-0	R1.	The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:	The Responsible Entity failed to include in their assessment one of the subrequirements.	The Responsible Entity failed to include in their assessment two of the subrequirements.	The Responsible Entity failed to include in their assessment three of the subrequirements.	The Responsible Entity failed to include in their assessment four or more of the subrequirements.
FAC-002-0	R1.1.	Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evaluation.
FAC-002-0	R1.2.	Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the ensurance of compliance.
FAC-002-0	R1.3.	Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evidence of coordination.
FAC-002-0	R1.4.	Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance in accordance with Reliability Standard TPL-001-0.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evidence of the studies.

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-002-0	R1.5.	Documentation that the assessment included study assumptions, system performance, and alternatives considered, and jointly coordinated recommendations.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the documentation.
FAC-002-0	R2.	The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) Regional Reliability Organization(s) and NERC on request (within 30 calendar days).	The responsible entity provided the documentation more than 30 calendar days, but not more than 45 calendar days, after a request.	The responsible entity provided the documentation more than 45 calendar days, but not more than 60 calendar days, after a request.	The responsible entity provided the documentation more than 60 calendar days, but not more than 120 calendar days, after a request.	The responsible entity provided the documentation more than 120 calendar days after a request or was unable to provide the documentation.
FAC-003-1	R1.	The Transmission owner shall prepare, and keep current, a formal transmission vegetation management program (TVMP). The TVMP shall include the Transmission Owner's objectives, practices, approved procedures, and work Specifications. 1. ANSI A300, Tree Care Operations – Tree, Shrub, and Other Woody Plant Maintenance – Standard Practices, while not a requirement of this standard, is considered to be an industry best practice.	The applicable entity did not include and keep current one of the four required elements of its TVMP, as directed by the requirement.	The applicable entity did not include and keep current two of the four required elements of its TVMP, as directed by the requirement.	The applicable entity did not include and keep current three of the four required elements of its TVMP, as directed by the requirement.	The applicable entity did not include and keep current four of the four required elements of the TVMP, as directed by the requirement.
FAC-003-1	R1.1.	The TVMP shall define a schedule for and the type (aerial, ground) of	N/A	N/A	The applicable entity TVMP did	The applicable entity TVMP did

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ROW vegetation inspections. This schedule should be flexible enough to adjust for changing conditions. The inspection schedule shall be based on the anticipated growth of vegetation and any other environmental or operational factors that could impact the relationship of vegetation to the Transmission Owner's transmission lines.			not define a schedule, as directed by the requirement, or the type of ROW vegetation inspections, as directed by the requirement.	not define a schedule, as directed by the requirement, nor the type of ROW vegetation inspections, as directed by the requirement.
FAC-003-1	R1.2.	The Transmission Owner, in the TVMP, shall identify and document clearances between vegetation and any overhead, ungrounded supply conductors, taking into consideration transmission line voltage, the effects of ambient temperature on conductor sag under maximum design loading, and the effects of wind velocities on conductor sway. Specifically, the Transmission Owner shall establish clearances to be achieved at the time of vegetation management work identified herein as Clearance 1, and shall also establish and maintain a set of clearances identified herein as Clearance 2 to prevent flashover between vegetation and overhead ungrounded supply conductors.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission Owner's TVMP does not specify clearances.
FAC-003-1	R1.2.1.	Clearance 1 — The Transmission Owner shall determine and document appropriate clearance distances to be achieved at the time of transmission vegetation management work based upon local conditions and the expected time frame in which the	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission Owner's TVMP does not specify Clearance 1 values.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Owner plans to return for future vegetation management work. Local conditions may include, but are not limited to: operating voltage, appropriate vegetation management techniques, fire risk, reasonably anticipated tree and conductor movement, species types and growth rates, species failure characteristics, local climate and rainfall patterns, line terrain and elevation, location of the vegetation within the span, and worker approach distance requirements. Clearance 1 distances shall be greater than those defined by Clearance 2 below.				
FAC-003-1	R1.2.2.	Clearance 2 — The Transmission Owner shall determine and document specific radial clearances to be maintained between vegetation and conductors under all rated electrical operating conditions. These minimum clearance distances are necessary to prevent flashover between vegetation and conductors and will vary due to such factors as altitude and operating voltage. These Transmission Owner-specific minimum clearance distances shall be no less than those set forth in the Institute of Electrical and Electronics Engineers (IEEE) Standard 516-2003 (<i>Guide for Maintenance Methods on Energized Power Lines</i>) and as specified in its Section 4.2.2.3, Minimum Air Insulation Distances	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission Owner's TVMP does not specify Clearance 2 values.

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		without Tools in the Air Gap.				
FAC-003-1	R1.2.2.1.	Where transmission system transient overvoltage factors are not known, clearances shall be derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.	Not Applicable.	Not Applicable.	Not Applicable.	Where transmission system transient overvoltage factors are known, clearances were not derived from Table 5, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.
FAC-003-1	R1.2.2.2.	Where transmission system transient overvoltage factors are known, clearances shall be derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.	Not Applicable.	Not Applicable.	Not Applicable.	Where transmission system transient overvoltage factors are known, clearances were not derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.
FAC-003-1	R1.3.	All personnel directly involved in the design and implementation of the TVMP shall hold appropriate qualifications and training, as defined by the Transmission Owner, to perform their duties.	One or more persons directly involved in the design and implementation of the TVMP (but not more than 35% of the all personnel involved), did not	More than 35% of all personnel directly involved in the design and implementation of the TVMP (but not more than 70% of all personnel involved), did not	More than 70% of all personnel directly involved in the design and implementation of the TVMP (but not 100% of all personnel involved), did not	None of the persons directly involved in the design and implementation of the Transmission Owner's TVMP held appropriate qualifications and

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			hold appropriate qualifications and training to perform their duties.	hold appropriate qualifications and training to perform their duties.	hold appropriate qualifications and training to perform their duties.	training to perform their duties.
FAC-003-1	R1.4.	Each Transmission Owner shall develop mitigation measures to achieve sufficient clearances for the protection of the transmission facilities when it identifies locations on the ROW where the Transmission Owner is restricted from attaining the clearances specified in Requirement 1.2.1.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission Owner's TVMP does not include mitigation measures to achieve sufficient clearances where restrictions to the ROW are in effect.
FAC-003-1	R1.5.	Each Transmission Owner shall establish and document a process for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage. This is so that action (temporary reduction in line rating, switching line out of service, etc.) may be taken until the threat is relieved.	N/A	N/A	N/A	The applicable entity did not establish or did not document a process, as directed by the requirement.
FAC-003-1	R2.	The Transmission Owner shall create and implement an annual plan for vegetation management work to ensure the reliability of the system. The plan shall describe the methods used, such as manual clearing, mechanical clearing, herbicide treatment, or other actions. The plan should be flexible enough to adjust to changing conditions, taking into consideration anticipated growth of vegetation and all other	The Transmission Owner did not meet one of the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of	The Transmission Owner did not meet two of the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of	The Transmission Owner did not meet the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of	The Transmission Owner does not have an annual plan for vegetation management, or the Transmission Owner has not implemented the annual plan for vegetation management.

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		environmental factors that may have an impact on the reliability of the transmission systems. Adjustments to the plan shall be documented as they occur. The plan should take into consideration the time required to obtain permissions or permits from landowners or regulatory authorities. Each Transmission Owner shall have systems and procedures for documenting and tracking the planned vegetation management work and ensuring that the vegetation management work was completed according to work specifications.	adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the requirement.	adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the requirement.	adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the requirement.	
FAC-003-1	R3.	The Transmission Owner shall report quarterly to its RRO, or the RRO's designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation.	The Transmission Owner did not submit a quarterly report to its RRO and did not have any outages to report	The Transmission Owner did not report an outage specified as reportable in R3 to its RRO	The Transmission Owner did not report multiple outages specified as reportable in R3 to its RRO	The Transmission Owner did not report one or more outages specified as reportable in R3 to its RRO for two consecutive quarters
FAC-003-1	R3.1.	Multiple sustained outages on an individual line, if caused by the same vegetation, shall be reported as one outage regardless of the actual number of outages within a 24-hour period.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner failed to report, as a single outage, multiple sustained outages within a 24-hour period on an individual line, if caused by the same vegetation.
FAC-003-1	R3.2.	The Transmission Owner is not required to report to the RRO, or the	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner made

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		RRO's designee, certain sustained transmission line outages caused by vegetation: (1) Vegetation-related outages that result from vegetation falling into lines from outside the ROW that result from natural disasters shall not be considered reportable (examples of disasters that could create non-reportable outages include, but are not limited to, earthquakes, fires, tornados, hurricanes, landslides, wind shear, major storms as defined either by the Transmission Owner or an applicable regulatory body, ice storms, and floods), and (2) Vegetation-related outages due to human or animal activity shall not be considered reportable (examples of human or animal activity that could cause a non-reportable outage include, but are not limited to, logging, animal severing tree, vehicle contact with tree, arboricultural activities or horticultural or agricultural activities, or removal or digging of vegetation).				reports for outages not considered reportable based on the categories listed in this requirement.
FAC-003-1	R3.3.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, shall include at a minimum: the name of the circuit(s) outaged, the date, time and duration of the outage; a description of the cause of the outage; other pertinent comments; and any countermeasures taken by the Transmission Owner.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, did not include one of the required elements.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, did not include two of the required elements.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, did not include three of the required elements.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, did not include four or more of the required elements.

Complete Violation Severity Level Matrix (FAC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-003-1	R3.4.	An outage shall be categorized as one of the following:	Not applicable.	Not applicable.	Not applicable.	The outage was not classified in the correct category.
FAC-003-1	R3.4.1.	Category 1 — Grow-ins: Outages caused by vegetation growing into lines from vegetation inside and/or outside of the ROW;	Not applicable.	Not applicable.	Not applicable.	The outage was not classified in the correct category.
FAC-003-1	R3.4.2.	Category 2 — Fall-ins: Outages caused by vegetation falling into lines from inside the ROW;	Not applicable.	Not applicable.	Not applicable.	The outage was not classified in the correct category.
FAC-003-1	R3.4.3.	Category 3 — Fall-ins: Outages caused by vegetation falling into lines from outside the ROW.	Not applicable.	Not applicable.	Not applicable.	The outage was not classified in the correct category.
FAC-003-1	R4.	The RRO shall report the outage information provided to it by Transmission Owner's, as required by Requirement 3, quarterly to NERC, as well as any actions taken by the RRO as a result of any of the reported outages.	Not applicable.	Not applicable.	The RRO did not submit a quarterly report to NERC for a single quarter.	The RRO did not submit a quarterly report to NERC for more than two consecutive quarters.
FAC-008-1	R1.	The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generation Owner does not have a documented Facility Ratings Methodology for use in developing facility ratings.
FAC-008-1	R1.1.	A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.	The Facility Rating methodology respects the most limiting applicable Equipment Rating of the individual equipment that	Not applicable.	Not applicable.	The Transmission Owner or Generation Owner has failed to demonstrate that its Facility Rating Methodology

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			comprises that Facility but there is no statement in the documentation of the methodology that states this.			respects the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
FAC-008-1	R1.2.	The method by which the Rating (of major BES equipment that comprises a Facility) is determined.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner's or Generation Owner's Facility Ratings Methodology does not specify the manner in which a rating is determined.
FAC-008-1	R1.2.1.	The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.	Not applicable.	The Transmission Owner or Generator Owner has demonstrated that it has a Facility Rating Methodology that includes methods of rating BES equipment but the equipment rating methods don't address one of the applicable required devices.	The Transmission Owner or Generator Owner has demonstrated the existence of methods of rating equipment but the equipment rating methods don't address two of the applicable required devices.	The Transmission Owner or Generator Owner has demonstrated the existence of methods of rating equipment but the equipment rating methods don't address more than two of the applicable required devices.
FAC-008-1	R1.2.2.	The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.	Not applicable.	The Transmission Owner or Generator Owner's equipment Ratings	The Transmission Owner or Generator Owner's equipment Ratings	The Transmission Owner or Generator Owner's equipment Ratings

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				methodology does address a methodology for determining emergency ratings but fails to include a methodology for determining normal ratings for its BES equipment.	methodology fails to include a methodology for determining emergency ratings for of its BES equipment.	methodology fails to demonstrate the inclusion of any method for determining normal or emergency ratings for of its BES equipment.
FAC-008-1	R1.3.	Consideration of the following:	The rating methodology did not consider one of the sub requirements.	The rating methodology did not consider two of the sub requirements.	The rating methodology did not consider three of the sub requirements.	The rating methodology did not consider four or more of the sub requirements.
FAC-008-1	R1.3.1.	Ratings provided by equipment manufacturers.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate the existence (in its Facility Rating Methodology) of how it considered ratings provided by equipment manufacturers.
FAC-008-1	R1.3.2.	Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate how it considered design criteria in developing its equipment Ratings.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-008-1	R1.3.3.	Ambient conditions.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate how it considered ambient conditions in developing its equipment Ratings.
FAC-008-1	R1.3.4.	Operating limitations.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate how it considered operating limitations in developing its equipment Ratings.
FAC-008-1	R1.3.5.	Other assumptions.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate how it considered other assumptions in developing its equipment Ratings.
FAC-008-1	R2.	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have	The Transmission Owner or Generator Owner has made its Facility Ratings Methodology available to all required entities	The Transmission Owner or Generator Owner has not made its Facility Ratings Methodology available to one of the required	The Transmission Owner or Generator Owner fails to provide its Facility Ratings Methodology available to two or more of the	The Transmission Owner or Generator Owner has not made its Facility Rating Methodology available to any of the required entities

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.	but not within 15 business days of a request.	entities, but did not make the methodology available to all other required entities.	required entities.	in accordance with Requirement R2 within 60 business days of receipt of a request.
FAC-008-1	R3.	If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.	The responsible entity provided a response as required but took longer than 45 business days.	The responsible entity provided a response and the response indicated that a change will not be made to the Facility Ratings Methodology but did not indicate why no change will be made.	The responsible entity provided a response but the response did not indicate whether a change will be made to the Facility Ratings Methodology.	The responsible entity did not provide any evidence to demonstrate that it provided a response to a comment on its Facility Ratings Methodology in accordance with Requirement R3 within 90 business days.
FAC-009-1	R1.	The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology.	The Transmission Owner or Generator Owner developed Facility Ratings for all its solely owned and jointly owned Facilities, but the ratings weren't consistent with the associated Facility Rating Methodology in	The Transmission Owner or Generator Owner developed Facility Ratings for most, but not all of its solely and jointly owned Facilities following the associated Facility Ratings Methodology	The Transmission Owner or Generator Owner developed Facility Ratings following the associated Facility Ratings Methodology but failed to develop any Facility Ratings for a significant number of its solely and	The Transmission Owner or Generator Owner has failed to demonstrate that it developed any Facility Ratings using its Facility Rating Methodology

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			one minor area.	OR the Transmission Owner or Generator Owner developed Facility Ratings for all its solely and jointly owned Facilities but failed to follow the associated Facility Ratings Methodology in one significant area.	jointly owned Facilities OR the Transmission Owner or Generator Owner has developed Facility Ratings for all its solely owned and jointly owned Facilities, but failed to follow the associated Facility Ratings Methodology in more than one significant area.	
FAC-009-1	R2.	The Transmission Owner and Generator Owner shall each provide Facility Ratings for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities to its associated Reliability Coordinator(s), Planning Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities.	The Transmission Owner or Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to 15 calendar days.	The Transmission Owner or Generator Owner provided its Facility Ratings to all but one of the requesting entities.	The Transmission Owner or Generator Owner provided its Facility Ratings to two of the requesting entities.	The Transmission Owner or Generator Owner has provided its Facility Ratings to none of the requesting entities within 30 calendar days of the associated schedules.
FAC-010-2	R1	The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL	Not applicable.	The Planning Authority has a documented SOL Methodology for	The Planning Authority has a documented SOL Methodology for	The Planning Authority has a documented SOL Methodology for

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Methodology shall:		use in developing SOLs within its Planning Authority Area, but it does not address R1.2	use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	use in developing SOLs within its Planning Authority Area, but it does not address R1.1. OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
FAC-010-2	R1.1.	Be applicable for developing SOLs used in the planning horizon.	Not applicable.	Not applicable.	Not applicable.	Planning Authority SOL methodology is not applicable for developing SOL in the planning horizon.
FAC-010-2	R1.2.	State that SOLs shall not exceed associated Facility Ratings.	Not applicable.	Not applicable.	Not applicable.	Planning Authority SOL Methodology did not state that SOLs shall not exceed associated Facility Ratings
FAC-010-2	R1.3.	Include a description of how to identify the subset of SOLs that qualify as IROLs.	Not applicable.	Not applicable.	Not applicable.	Planning Authority SOL Methodology did not include a description of how to identify the subset of SOLs that qualify as IROLs.
FAC-010-2	R2.	The Planning Authority's SOL				

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Methodology shall include a requirement that SOLs provide BES performance consistent with the following				
FAC-010-2	R2.1.	In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority's methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.1.
FAC-010-2	R2.2.	Following the single Contingencies identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority's methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.2.
FAC-010-2	R2.2.1.	Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line,

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						transformer, or shunt device.
FAC-010-2	R2.2.2.	Loss of any generator, line, transformer, or shunt device without a Fault.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address the loss of any generator, line, transformer, or shunt device without a Fault.
FAC-010-2	R2.2.3.	Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
FAC-010-2	R2.3.	Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:	Not applicable.	Not applicable.	Not applicable.	The methodology does not include one or more of the following: 2.3.1. through 2.3.3.
FAC-010-2	R2.3.1.	Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.	Not applicable.	Not applicable.	Not applicable.	The SOL Methodology does not provide that starting with all Facilities in service, the system's response to a single Contingency may include planned or controlled

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.
FAC-010-2	R2.3.2.	System reconfiguration through manual or automatic control or protection actions.	Not applicable.	Not applicable.	Not applicable.	The SOL Methodology does not provide that starting with all Facilities in service, the system's response to a single Contingency may include System reconfiguration through manual or automatic control or protection actions.
FAC-010-2	R2.4.	To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.	Not applicable.	Not applicable.	Not applicable.	The SOL Methodology does not provide that in order to prepare for the next Contingency, system adjustments may be made, including changes to generation, uses

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						of the transmission system, and the transmission system topology.
FAC-010-2	R2.5.	Starting with all Facilities in service and following any of the multiple Contingencies identified in Reliability Standard TPL-003 the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.	Not applicable.	Not applicable.	Not applicable.	The SOL methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.5.
FAC-010-2	R2.6.	In determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2, the following shall be acceptable:	Not applicable.	Not applicable.	Not applicable.	Not applicable.
FAC-010-2	R2.6.1.	Planned or controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers.	Not applicable.	Not applicable.	Not applicable.	The SOL Methodology does not provide that in determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2,

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Planned or controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers shall be acceptable.
FAC-010-2	R3.	The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.6.
FAC-010-2	R3.1.	Study model (must include at least the entire Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).	Not applicable.	Not applicable.	Not applicable.	The methodology does not include a study model that includes the entire Planning Authority Area, and the critical modeling details of other Planning Authority Areas that would

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						impact the facility or facilities under study.
FAC-010-2	R3.2.	Selection of applicable Contingencies.	Not applicable.	Not applicable.	Not applicable.	The methodology does not include the selection of applicable Contingencies.
FAC-010-2	R3.3	Level of detail of system models used to determine SOLs.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe the level of detail of system models used to determine SOLs.
FAC-010-2	R3.4.	Allowed uses of Special Protection Systems or Remedial Action Plans.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe the allowed uses of Special Protection Systems or Remedial Action Plans.
FAC-010-2	R3.5.	Anticipated transmission system configuration, generation dispatch and Load level.	Not applicable.	Not applicable.	Not applicable.	The methodology does not include the description of anticipated transmission system configuration, generation dispatch and Load level.
FAC-010-2	R3.6.	Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating	Not applicable.	Not applicable.	Not applicable.	The methodology does not include a description of the

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Limit (IROL) and criteria for developing any associated IROL T _v .				criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T _v .
FAC-010-2	R4.	The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:	<p>One or both of the following:</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities.</p> <p>For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>One of the following:</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change.</p> <p>OR</p>	<p>One of the following:</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change.</p> <p>OR</p> <p>The Planning Authority issued its</p>	<p>One of the following:</p> <p>The Planning Authority failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities.</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was</p>

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change.</p> <p>OR</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>provided 90 calendar days or more after the effectiveness of the change.</p> <p>OR</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change.</p> <p>OR</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology,</p>

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>
FAC-010-2	R4.1.	Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not issue its SOL Methodology and any change to that methodology, prior to the effectiveness of the change, to each adjacent Planning Authority and each Planning

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Authority that indicated it has a reliability-related need for the methodology.
FAC-010-2	R4.2.	Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not issue its SOL Methodology and any change to that methodology, prior to the effectiveness of the change, to each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.
FAC-010-2	R4.3.	Each Transmission Planner that works in the Planning Authority's Planning Authority Area.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not issue its SOL Methodology and any change to that methodology, prior to the effectiveness of the change, to each Transmission Planner that works in the Planning Authority's

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Planning Authority Area prior to the effectiveness of the change.
FAC-010-2	R5.	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.
FAC-011-2	R1.	The Reliability Coordinator shall have a documented methodology for	Not applicable.	The Reliability Coordinator has a	The Reliability Coordinator has a	The Reliability Coordinator has a

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:		documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
FAC-011-2	R1.1.	Be applicable for developing SOLs used in the operations horizon.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator's SOL methodology is not applicable for developing SOL in the operations horizon.
FAC-011-2	R1.2.	State that SOLs shall not exceed associated Facility Ratings.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator's SOL Methodology did not state that SOLs shall not exceed associated Facility Ratings
FAC-011-2	R1.3	Include a description of how to identify the subset of SOLs that	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator's SOL

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		qualify as IROLs				Methodology did not include a description of how to identify the subset of SOLs that qualify as IROLs.
FAC-011-2	R2.	The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:				
FAC-011-2	R2.1.	In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.	Not applicable.	Not applicable.	Not applicable.	The SOL methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.1.
FAC-011-2	R2.2.	Following the single Contingencies1 identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.	Not applicable.	Not applicable.	Not applicable.	The SOL methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.2.
FAC-011-2	R2.2.1.	Single line to ground or 3-phase Fault (whichever is more severe), with	Not applicable.	Not applicable.	Not applicable.	The methodology does not require

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Normal Clearing, on any Faulted generator, line, transformer, or shunt device				that SOLs provide BES performance consistent with: single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.
FAC-011-2	R2.2.2.	Loss of any generator, line, transformer, or shunt device without a Fault.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address the loss of any generator, line, transformer, or shunt device without a Fault.
FAC-011-2	R2.2.3.	Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
FAC-011-2	R2.3.	In determining the system's response to a single Contingency, the following shall be acceptable:	Not applicable.	Not applicable.	Not applicable.	The methodology does not include one or more of the following 2.3.1. through 2.3.3.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-011-2	R2.3.1.	Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address that, in determining the systems response to a single contingency, Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area is acceptable.
FAC-011-2	R2.3.2.	Interruption of other network customers, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time operating conditions are more adverse than anticipated in the corresponding studies	Not applicable.	Not applicable.	Not applicable.	The methodology does not address that, in determining the systems response to a single contingency, Interruption of other network customers is acceptable, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						operating conditions are more adverse than anticipated in the corresponding studies.
FAC-011-2	R2.3.3.	System reconfiguration through manual or automatic control or protection actions.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address that, in determining the systems response to a single contingency, system reconfiguration through manual or automatic control or protection actions is acceptable.
FAC-011-2	R2.4.	To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.	Not applicable.	Not applicable.	Not applicable.	The methodology does not provide that to prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.
FAC-011-2	R3.	The Reliability Coordinator's methodology for determining SOLs,	The Reliability Coordinator has a	The Reliability Coordinator has a	The Reliability Coordinator has a	The Reliability Coordinator has a

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.7.
FAC-011-2	R3.1.	Study model (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)	Not applicable.	Not applicable.	Not applicable.	The methodology does not include a description of the study model to be used which must include the entire Reliability Coordinator area, and the critical details of other Reliability Coordinator areas that would impact the facility or facilities under study
FAC-011-2	R3.2.	Selection of applicable Contingencies	Not applicable.	Not applicable.	Not applicable.	The methodology does not include the selection of applicable Contingencies.
FAC-011-2	R3.3.	A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use	Not applicable.	Not applicable.	Not applicable.	The methodology does not include a description of a process for determining which of the stability

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		in the operating horizon given the actual or expected system conditions.				limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.
FAC-011-2	R3.3.1.	This process shall address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple contingencies	Not applicable.	Not applicable.	Not applicable.	The methodology for determining SOL's does not address the need to modify the limits described in R3.3, the list of limits, or the list of associated multiple contingencies.
FAC-011-2	R3.4.	Level of detail of system models used to determine SOLs.	Not applicable.	Not applicable.	Not applicable.	Methodology does not describe the level of detail of system models used to determine SOLs.
FAC-011-2	R3.5.	Allowed uses of Special Protection Systems or Remedial Action Plans.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe the allowed uses of Special Protection

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems or Remedial Action Plans.
FAC-011-2	R3.6.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe the anticipated transmission system configuration, generation dispatch and Load level.	
FAC-011-2	R3.7.	Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v .	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit and criteria for developing any associated IROL T_v .
FAC-011-2	R4	The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:	One or both of the following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the	One of the two following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities	One of the following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>required entities.</p> <p>For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR</p> <p>The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR</p> <p>The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR</p> <p>The Reliability Coordinator issued its SOL Methodology and changes to that</p>	<p>entities.</p> <p>The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change.</p> <p>OR</p> <p>The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days</p>

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>after the effectiveness of the change.</p> <p>OR</p> <p>The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change.</p> <p>OR</p> <p>The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology,</p>

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the changed methodology was provided up to 30 calendar days after the effectiveness of the change
FAC-011-2	R4.1.	Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator did not issue its SOL Methodology or any changes to that methodology to each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.
FAC-011-2	R4.2.	Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator did not issue its SOL Methodology or any changes to that methodology to each Planning Authority or Transmission Planner that models any portion of the Reliability Coordinator's Reliability

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Coordinator Area.
FAC-011-2	R4.3.	Each Transmission Operator that operates in the Reliability Coordinator Area.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator did not issue its SOL Methodology or any changes to that methodology to each Transmission Operator that operates in the Reliability Coordinator Area.
FAC-011-2	R5.	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.
FAC-013-1	R1.	The Reliability Coordinator and Planning Authority shall each establish a set of inter-regional and intra-regional Transfer Capabilities that is consistent with its current Transfer Capability Methodology.	The Reliability Coordinator or Planning Authority has established a set of Transfer Capabilities, but one or more Transfer Capabilities, but not more than 25% of all Transfer Capabilities required to be established, are not consistent with the current Transfer Capability Methodology.	The Reliability Coordinator or Planning Authority has established a set of Transfer Capabilities, but more than 25% of those Transfer Capabilities, but not more than 50% of all Transfer Capabilities required to be established, are not consistent with the current Transfer Capability Methodology.	The Reliability Coordinator or Planning Authority has established a set of Transfer Capabilities, but more than 50% of those Transfer Capabilities, but not more than 75% of all Transfer Capabilities required to be established, are not consistent with the current Transfer Capability Methodology.	The Reliability Coordinator or Planning Authority has established a set of Transfer Capabilities, but more than 75% of those Transfer Capabilities are not consistent with the current Transfer Capability Methodology OR The Reliability Coordinator or Planning Authority has not established a set of Transfer Capabilities.
FAC-013-1	R2.	The Reliability Coordinator and Planning Authority shall each provide its inter-regional and intra-regional	The Reliability Coordinator or Planning Authority	The Reliability Coordinator or Planning Authority	The Reliability Coordinator or Planning Authority	The Reliability Coordinator or Planning Authority

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transfer Capabilities to those entities that have a reliability-related need for such Transfer Capabilities and make a written request that includes a schedule for delivery of such Transfer Capabilities as follows:	has provided its Transfer Capabilities but missed meeting one schedule by up to 15 calendar days.	has provided its Transfer Capabilities but missed meeting two schedules.	has provided its Transfer Capabilities but missed meeting more than two schedules.	has provided its Transfer Capabilities but missed meeting all schedules within 30 calendar days of the associated schedules.
FAC-013-1	R2.1.	The Reliability Coordinator shall provide its Transfer Capabilities to its associated Regional Reliability Organization(s), to its adjacent Reliability Coordinators, and to the Transmission Operators, Transmission Service Providers and Planning Authorities that work in its Reliability Coordinator Area.	Not applicable.	The Reliability Coordinator provided its Transfer Capabilities to all but one of the required entities.	The Reliability Coordinator failed to provide its Transfer Capabilities to more than one of the required entities.	The Reliability Coordinator provided its Transfer Capabilities to none of the required entities.
FAC-013-1	R2.2.	The Planning Authority shall provide its Transfer Capabilities to its associated Reliability Coordinator(s) and Regional Reliability Organization(s), and to the Transmission Planners and Transmission Service Provider(s) that work in its Planning Authority Area.	Not applicable.	The Planning Authority provided its Transfer Capabilities to all but one of the required entities.	The Planning Authority failed to provide its Transfer Capabilities to more than one of the required entities.	The Planning Authority provided its Transfer Capabilities to none of the required entities.
FAC-014-2	R1.	The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.	There are SOLs, for the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs for the Reliability Coordinator Area, but one or more of these the SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-014-2	R2.	The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 75% or more of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)
FAC-014-2	R3.	The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology	There are SOLs, for the Planning Coordinator Area, but from 1% up to, but less than, 25% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are SOLs, for the Planning Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are SOLs for the Planning Coordinator Area, but 10% or more, but less than 75% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are SOLs, for the Planning Coordinator Area, but 75% or more of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)
FAC-014-2	R4.	The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology.	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but up to 25% of these SOLs are inconsistent with the Planning Coordinator's SOL	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Planning Coordinator's SOL	The Transmission Planner has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Planning Coordinator's SOL	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but one or more of these SOLs are inconsistent with the Planning Coordinator's SOL

Complete Violation Severity Level Matrix (FAC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Methodology. (R4)	Methodology. (R4)	Methodology. (R4)	Methodology. (R4)
FAC-014-2	R5.	The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows	The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules by less than 15 calendar days. (R5)	One of the following: The responsible entity provided its SOLs to all but one of the requesting entities within the schedules provided. (R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules for 15 or more but less than 30 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.4	One of the following: The responsible entity provided its SOLs to all but two of the requesting entities within the schedules provided. (R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules for 30 or more but less than 45 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.3	One of the following: The responsible entity failed to provide its SOLs to more than two of the requesting entities within 45 calendar days of the associated schedules. (R5) OR The supporting information provided with the IROLs does not address 5.1.1 and 5.1.2.
FAC-014-2	R5.1.	The Reliability Coordinator shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Reliability Coordinators and Reliability Coordinators who indicate	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator did not provide its SOLs (including the subset of SOLs that

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		a reliability-related need for those limits, and to the Transmission Operators, Transmission Planners, Transmission Service Providers and Planning Authorities within its Reliability Coordinator Area. For each IROL, the Reliability Coordinator shall provide the following supporting information				are IROLs) to adjacent Reliability Coordinators and Reliability Coordinators who indicate a reliability-related need for those limits, and to the Transmission Operators, Transmission Planners, Transmission Service Providers and Planning Authorities within its Reliability Coordinator Area.
FAC-014-2	R5.1.1.	Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL	Not applicable.	Not applicable.	Not applicable.	For any IROL, the Reliability Coordinator did not provide the Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL.
FAC-014-2	R5.1.2.	The value of the IROL and its associated Tv.	Not applicable.	Not applicable.	Not applicable.	For any IROL, the Reliability Coordinator did not provide the value

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						of the IROL and its associated Tv.
FAC-014-2	R5.1.3.	The associated Contingency (ies).	Not applicable.	Not applicable.	Not applicable.	For any IROL, the Reliability Coordinator did not provide the associated Contingency(ies).
FAC-014-2	R5.1.4.	The type of limitation represented by the IROL (e.g., voltage collapse, angular stability).	Not applicable.	Not applicable.	Not applicable.	For any IROL, the Reliability Coordinator did not provide the type of limitation represented by the IROL (e.g., voltage collapse, angular stability).
FAC-014-2	R5.2.	The Transmission Operator shall provide any SOLs it developed to its Reliability Coordinator and to the Transmission Service Providers that share its portion of the Reliability Coordinator Area.	Not applicable.	Not applicable.	Not applicable.	The Transmission Operator did not provide the complete set of SOLs it developed to its Reliability Coordinator and to the Transmission Service Providers that share its portion of the Reliability Coordinator Area.
FAC-014-2	R5.3.	The Planning Authority shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Planning Authorities, and to	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not provide its complete set of

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Planners, Transmission Service Providers, Transmission Operators and Reliability Coordinators that work within its Planning Authority Area.				SOLs (including the subset of SOLs that are IROLs) to adjacent Planning Authorities, and to Transmission Planners, Transmission Service Providers, Transmission Operators and Reliability Coordinators that work within its Planning Authority Area.
FAC-014-2	R5.4.	The Transmission Planner shall provide its SOLs (including the subset of SOLs that are IROLs) to its Planning Authority, Reliability Coordinators, Transmission Operators, and Transmission Service Providers that work within its Transmission Planning Area and to adjacent Transmission Planners.	Not applicable.	Not applicable.	Not applicable.	The Transmission Planner did not provide its complete set of SOLs (including the subset of SOLs that are IROLs) to its Planning Authority, Reliability Coordinators, Transmission Operators, and Transmission Service Providers that work within its Transmission Planning Area and to adjacent

**Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Transmission Planners.
FAC-014-2	R6.	The Planning Authority shall identify the subset of multiple contingencies (if any), from Reliability Standard TPL-003 which result in stability limits.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not identify the subset of multiple contingencies which result in stability limits. (R6)
FAC-014-2	R6.1.	The Planning Authority shall provide this list of multiple contingencies and the associated stability limits to the Reliability Coordinators that monitor the facilities associated with these contingencies and limits.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not identify the subset of multiple contingencies, from TPL-003 that resulted in stability limits and provide the complete list of multiple contingencies and the associated stability limits to the Reliability Coordinators that monitor the facilities associated with these contingencies and limits.
FAC-014-2	R6.2.	If the Planning Authority does not identify any stability-related multiple contingencies, the Planning Authority	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not notify the

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall so notify the Reliability Coordinator.				Reliability Coordinator that it did not identify any stability-related multiple contingencies,

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-001-3	R1.	The Load-Serving, Purchasing-Selling Entity shall ensure that Arranged Interchange is submitted to the Interchange Authority for:	The Load-Serving, Purchasing-Selling Entity experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)
INT-001-3	R1.1.	All Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.
INT-001-3	R2.	The Sink Balancing Authority shall ensure that Arranged Interchange is submitted to the Interchange Authority:	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)
INT-001-3	R2.1.	If a Purchasing-Selling Entity is not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.
INT-001-3	R2.2.	For each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.
INT-003-2	R1.	Each Receiving Balancing Authority shall confirm Interchange Schedules with the Sending Balancing Authority prior to implementation in the Balancing Authority's ACE equation.	There shall be a separate Lower VSL, if either of the following conditions exists: One instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. One instance of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	There shall be a separate Moderate VSL, if either of the following conditions exists: Two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Two instances of not coordinating the Interchange	There shall be a separate High VSL, if either of the following conditions exists: Three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Three instances of not coordinating the Interchange	There shall be a separate Severe VSL, if either of the following conditions exists: Four or more instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Four or more instances of not coordinating the Interchange

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	Schedule with the Transmission Operator of the HVDC tie as specified in R1.2
INT-003-2	R1.1.	The Sending Balancing Authority and Receiving Balancing Authority shall agree on Interchange as received from the Interchange Authority, including:	The Balancing Authority experienced one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-2	R1.1.1.	Interchange Schedule start and end time.	The Balancing Authority experienced one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-2	R1.1.2.	Energy profile.	The Balancing Authority experienced one instance of entering a schedule into its ACE equation	The Balancing Authority experienced two instances of entering a schedule into its ACE equation	The Balancing Authority experienced three instances of entering a schedule into its ACE equation	The Balancing Authority experienced four instances of entering a schedule into its ACE equation

Complete Violation Severity Level Matrix (INT) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-2	R1.2.	If a high voltage direct current (HVDC) tie is on the Scheduling Path, then the Sending Balancing Authorities and Receiving Balancing Authorities shall coordinate the Interchange Schedule with the Transmission Operator of the HVDC tie.	The sending or receiving Balancing Authority experienced one instance of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced two instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced three instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced four instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2
INT-004-2	R1.	At such time as the reliability event allows for the reloading of the transaction, the entity that initiated the curtailment shall release the limit on the Interchange Transaction tag to allow reloading the transaction and shall communicate the release of the limit to the Sink Balancing Authority.	The entity that initiated the curtailment failed to communicate the transaction reload to the Sink Balancing Authority	The entity that initiated the curtailment failed to reload the transaction and failed to communicate to the Sink Balancing Authority	N/A	N/A
INT-004-2	R2.	The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs:	The Purchase-Selling entity failed to update the tags when required less than 25% of times it was required, as determined in R2.1, R2.2, or R2.3.	The Purchase-Selling entity failed to update the tags when required 25% or more and less than 50% of the times it was required, as determined in R2.1, R2.2, or R2.3.	The Purchase-Selling entity failed to update the tags when required 50% or more but less than 75% of the times it was required, as determined in R2.1, R2.2, or R2.3.	The Purchase-Selling entity failed to update the tags when required 75% or more of the times it was required, as determined in R2.1, R2.2, or R2.3.
INT-004-2	R2.1.	The average energy profile in an hour is greater than 250 MW	The Purchase-Selling entity failed to update	The Purchase-Selling entity failed to update	The Purchase-Selling entity failed to update	The Purchase-Selling entity failed to update

Complete Violation Severity Level Matrix (INT) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +10%.	the tags when required less than 25% of times it was required.	the tags when required 25% or more and less than 50% of the times it was required.	the tags when required 50% or more but less than 75% of the times it was required.	the tags when required 75% or more of the times it was required.
INT-004-2	R2.2.	The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +25 megawatt-hours.	The Purchase-Selling entity failed to update the tags when required less than 25% of times it was required.	The Purchase-Selling entity failed to update the tags when required 25% or more and less than 50% of the times it was required.	The Purchase-Selling entity failed to update the tags when required 50% or more but less than 75% of the times it was required.	The Purchase-Selling entity failed to update the tags when required 75% or more of the times it was required.
INT-004-2	R2.3.	A Reliability Coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons.	The Purchase-Selling entity failed to update the tags when required less than 25% of times it was required.	The Purchase-Selling entity failed to update the tags when required 25% or more and less than 50% of the times it was required.	The Purchase-Selling entity failed to update the tags when required 50% or more but less than 75% of the times it was required.	The Purchase-Selling entity failed to update the tags when required 75% or more of the times it was required.
INT-005-2	R1.	Prior to the expiration of the time period defined in the Timing Table, Column A, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment to all reliability entities involved in the Interchange.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities
INT-005-2	R1.1.	When a Balancing Authority or Reliability Coordinator initiates a Curtailment to Confirmed or Implemented Interchange for reliability, the Interchange	The Interchange Authority experienced one occurrence of not distributing information to all	The Interchange Authority experienced two occurrences of not distributing information to all	The Interchange Authority experienced three occurrences of not distributing information to all	The Interchange Authority experienced four occurrences of not distributing information to all

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authority shall distribute the Arranged Interchange information for reliability assessment only to the Source Balancing Authority and the Sink Balancing Authority.	involved reliability entities.	involved reliability entities	involved reliability entities	involved reliability entities
INT-006-2	R1.	Prior to the expiration of the reliability assessment period defined in the Timing Table, Column B, the Balancing Authority and Transmission Service Provider shall respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	The Responsible Entity failed on one occasion to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	The Responsible Entity failed on two occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	The Responsible Entity failed on three occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	The Responsible Entity failed on four occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.
INT-006-2	R1.1.	Each involved Balancing Authority shall evaluate the Arranged Interchange with respect to:	The Balancing Authority failed to evaluate arranged interchange with respect to one of the requirements in the 3 sub-components.	N/A	The Balancing Authority failed to evaluate arranged interchange with respect to two of the requirements in the 3 sub-components.	The Balancing Authority failed to evaluate arranged interchange with respect to three of the requirements in the 3 sub-components.
INT-006-2	R1.1.1.	Energy profile (ability to support the magnitude of the Interchange).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Energy profile (ability to support the magnitude of the Interchange).
INT-006-2	R1.1.2.	Ramp (ability of generation maneuverability to accommodate).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Ramp (ability of generation maneuverability to accommodate).

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-006-2	R1.1.3.	Scheduling path (proper connectivity of Adjacent Balancing Authorities).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Scheduling path (proper connectivity of Adjacent Balancing Authorities).
INT-006-2	R1.2.	Each involved Transmission Service Provider shall confirm that the transmission service arrangements associated with the Arranged Interchange have adjacent Transmission Service Provider connectivity, are valid and prevailing transmission system limits will not be violated.	The Transmission Service Provider experienced one instance of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experienced two instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experienced three instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experience four instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.
INT-007-1	R1.	The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:	The Interchange Authority failed to verify one time, as indicated in R1.1, R1.2, R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed	The Interchange Authority failed to verify two times, as indicated in R1.1, R1.2, R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed	The Interchange Authority failed to verify three times, as indicated in R1.1, R1.2, R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed	The Interchange Authority failed to verify four times, as indicated in R1.1, R1.2, R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interchange.	Interchange.	Interchange.	Interchange.
INT-007-1	R1.1.	Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.2.	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.	The following are defined:	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.1.	Generation source and load sink.	The Interchange Authority failed to	The Interchange Authority failed to	The Interchange Authority failed to	The Interchange Authority failed to

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.2.	Megawatt profile.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.3.	Ramp start and stop times.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.4.	Interchange duration.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.4.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval, with minor exception and is substantially compliant with the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval, with some exception and is mostly compliant with the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval but was substantially deficient in meeting the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment did not provide approval and failed to meet the requirement.
INT-008-2	R1.	Prior to the expiration of the time period defined in the Timing Table, Column C, the Interchange Authority shall distribute to all Balancing Authorities (including Balancing Authorities on both sides of a direct current tie), Transmission Service Providers and Purchasing-Selling Entities involved in the Arranged Interchange whether or not the Arranged Interchange has transitioned to a Confirmed	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as delineated in R1.1, R1.1.1 or R1.1.2.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities or no evidence provided.

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Interchange.				
INT-008-2	R1.1.	For Confirmed Interchange, the Interchange Authority shall also communicate:	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-008-2	R1.1.1.	Start and stop times, ramps, and megawatt profile to Balancing Authorities.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-008-2	R1.1.2.	Necessary Interchange information to NERC-identified reliability analysis services.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-009-1	R1.	The Balancing Authority shall implement Confirmed Interchange as received from the Interchange Authority.	The Balancing Authority experienced one occurrence of not implementing a Confirmed Interchange as received from the Interchange Authority.	The Balancing Authority experienced two occurrences of not implementing a Confirmed Interchange as received from the Interchange Authority.	The Balancing Authority experienced three occurrences of not implementing a Confirmed Interchange as received from the Interchange Authority.	The Balancing Authority experienced four occurrences of not implementing a Confirmed Interchange as received from the Interchange Authority.

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-010-1	R1.	The Balancing Authority that experiences a loss of resources covered by an energy sharing agreement shall ensure that a request for an Arranged Interchange is submitted with a start time no more than 60 minutes beyond the resource loss. If the use of the energy sharing agreement does not exceed 60 minutes from the time of the resource loss, no request for Arranged Interchange is required.	The Balancing Authority that experienced a loss of resource covered by an energy sharing agreement failed one time to submit a request for an Arranged Interchange within the specified time period.	The Balancing Authority that experienced a loss of resource covered by an energy sharing agreement failed two times to submit a request for an Arranged Interchange within the specified time period.	The Balancing Authority that experienced a loss of resource covered by an energy sharing agreement failed three times to submit a request for an Arranged Interchange within the specified time period.	The Balancing Authority that experienced a loss of resource covered by an energy sharing agreement failed four or more times to submit a request for an Arranged Interchange within the specified time period.
INT-010-1	R2.	For a modification to an existing Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit the modified Arranged Interchange reflecting that modification within 60 minutes of the initiation of the event.	The Reliability Coordinator failed one time to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed one time to submit the modified schedule as directed.	The Reliability Coordinator failed two times to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed two times to submit the modified schedule as directed.	The Reliability Coordinator failed three times to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed three times to submit the modified schedule as directed.	The Reliability Coordinator failed four times to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed four times to submit the modified schedule as directed.
INT-010-1	R3.	For a new Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit an Arranged Interchange reflecting that Interchange schedule within 60 minutes of	The Reliability Coordinator failed one time to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed one time to submit a schedule as directed.	The Reliability Coordinator failed two times to direct the submittal of a new or modified Arranged Interchange ; or the Balancing Authority failed two times to submit a schedule as directed.	The Reliability Coordinator failed three times to direct the submittal of a new or modified Arranged Interchange ; or the Balancing Authority failed three times to submit a schedule as directed.	The Reliability Coordinator failed four times to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed four times or more to submit a schedule as directed.

***Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards***

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the initiation of the event.				

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
IRO-001-1.1	R1.	Each Regional Reliability Organization, subregion, or interregional coordinating group shall establish one or more Reliability Coordinators to continuously assess transmission reliability and coordinate emergency operations among the operating entities within the region and across the regional boundaries.	The RRO, subregion or interregional coordinating group did not communicate the assignment of the Reliability Coordinators to operating entities clearly.	The RRO, subregion or interregional coordinating group did not clearly identify the coordination of Reliability Coordinator areas within the region.	The RRO, subregion or interregional coordinating group did not coordinate assignment of the Reliability Coordinators across regional boundaries.	The RRO, subregion or interregional coordinating group did not assign any Reliability Coordinators.
IRO-001-1.1	R2.	The Reliability Coordinator shall comply with a regional reliability plan approved by the NERC Operating Committee.	The Reliability Coordinator has failed to follow the administrative portions of its regional reliability plan.	The Reliability Coordinator has failed to follow steps in its regional reliability plan that requires operator interventions or actions.	The Reliability Coordinator does not have a regional reliability plan approved by the NERC OC.	The Reliability Coordinator does not have an unapproved regional reliability plan.
IRO-001-1.1	R3.	The Reliability Coordinator shall have clear decision-making authority to act and to direct actions to be taken by Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities within its Reliability Coordinator Area to preserve the integrity and reliability of the Bulk Electric System. These actions shall be taken without delay, but no longer than 30 minutes.	N/A	N/A	The Reliability Coordinator cannot demonstrate that it has clear authority to act or direct actions to preserve transmission security and reliability of the Bulk Electric System.	The Reliability Coordinator failed to take or direct to preserve the reliability and security of the Bulk Electric System within 30 minutes of identifying those actions.
IRO-001-1.1	R4.	Reliability Coordinators that delegate tasks to other entities shall have formal	1. Less than 25% of the tasks are not	1. More than 25% but 50% or less of	1. More than 50% but 75% or less of	1. There is no formal operating agreement

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		operating agreements with each entity to which tasks are delegated. The Reliability Coordinator shall verify that all delegated tasks are understood, communicated, and addressed within its Reliability Coordinator Area. All responsibilities for complying with NERC and regional standards applicable to Reliability Coordinators shall remain with the Reliability Coordinator.	documented in the agreement or 2. Less than 25% of the tasks are not performed according to the agreement.	the tasks are not documented in the agreement or 2. More than 25% but 50% or less of the tasks are not performed according to the agreement.	the tasks are not documented in the agreement or 2. More than 50% but 75% or less of the tasks are not performed according to the agreement.	for tasks delegated by the Reliability Coordinator, 2. More than 75% of the tasks are not documented in the agreement or 3. More than 75% of the tasks are not performed according to the agreement.
IRO-001-1.1	R5.	The Reliability Coordinator shall list within its reliability plan all entities to which the Reliability Coordinator has delegated required tasks.	25% or less of the delegate entities are not identified in the reliability plan.	More than 25% but 50% or less of the delegate entities are not identified in the reliability plan.	More than 50% but 75% or less of the delegate entities are not identified in the reliability plan.	1. There is no reliability plan or 2. More than 75% of the delegate entities are not identified in the reliability plan.
IRO-001-1.1	R6.	The Reliability Coordinator shall verify that all delegated tasks are carried out by NERC-certified Reliability Coordinator operating personnel.	N/A	1. The Reliability Coordinator has failed to demonstrate at least one delegated task was performed by NERC certified Reliability Coordinator operating personnel or 2. The Reliability Coordinator did not require the delegate entity to have NERC certified Reliability Coordinator operating	1. The Reliability Coordinator has failed to demonstrate at least one delegated task was performed by NERC certified Reliability Coordinator operating personnel and did not require the delegate entity to have NERC certified Reliability Coordinator operating personnel or 2. The Reliability Coordinator has	The Reliability Coordinator has failed to demonstrate any delegated tasks were performed by NERC certified Reliability Coordinator operating personnel and did not require the delegate entity to have NERC certified Reliability Coordinator operating personnel.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				personnel.	failed to demonstrate at least two delegated task were performed by NERC certified Reliability Coordinator operating personnel.	
IRO-001-1.1	R7.	The Reliability Coordinator shall have clear, comprehensive coordination agreements with adjacent Reliability Coordinators to ensure that System Operating Limit or Interconnection Reliability Operating Limit violation mitigation requiring actions in adjacent Reliability Coordinator Areas are coordinated.	The Reliability Coordinator has demonstrated the existence of coordination agreements with adjacent Reliability Coordinators but the agreements are not clear or comprehensive.	The Reliability Coordinator has demonstrated the existence of the coordination agreements with adjacent Reliability Coordinators but the agreements do not coordinate actions required in the adjacent Reliability Coordinator to mitigate SOL or IROL violations in its own Reliability Coordinator area.	The Reliability Coordinator has demonstrated the existence of the coordination agreements with adjacent Reliability Coordinators but the agreements do not coordinate actions required in the adjacent Reliability Coordinator to mitigate SOL and IROL violations in its own Reliability Coordinator area.	The Reliability Coordinator has failed to demonstrate the existence of any coordination agreements with adjacent Reliability Coordinators.
IRO-001-1.1	R8.	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities did not follow

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.	Entities, and Purchasing-Selling Entities followed the Reliability Coordinators directive with a delay not caused by equipment problems but did not notify the Reliability Coordinator of the delay.	Entities, and Purchasing-Selling Entities followed the Reliability Coordinators directive with a delay not caused by equipment problems and did not notify the Reliability Coordinator of the delay.	Entities, and Purchasing-Selling Entities followed the majority of the Reliability Coordinators directive and did not notify the Reliability Coordinator that it could not fully follow the directive because it would violate safety, equipment, statutory or regulatory requirements.	the Reliability Coordinators directive and did not notify the Reliability Coordinator that it could not follow the directive because it would violate safety, equipment, statutory or regulatory requirements.
IRO-001-1.1	R9.	The Reliability Coordinator shall act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of any other entity.	N/A	N/A	N/A	The Reliability Coordinator did not act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of one or more other entities.
IRO-002-1	R1.	Each Reliability Coordinator shall have adequate communications facilities (voice and data links) to appropriate entities within its Reliability Coordinator Area. These communications facilities shall be staffed and available to act in addressing a real-time emergency	The Reliability Coordinator has demonstrated communication facilities for both voice and data exist to all appropriate entities and that	The Reliability Coordinator has failed to demonstrate that is has: 1) Voice communication links with one	The Reliability Coordinator has failed to demonstrate that is has: 1) Voice communication links with two	The Reliability Coordinator has failed to demonstrate that is has: 1) Voice communication links with more than two appropriate entities or

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		condition.	they are staffed and available but they are less than adequate.	appropriate entity or 2) Data links with one appropriate entity.	appropriate entities or 2) Data links with two appropriate entities.	2) Data links with more than two appropriate entities or 3) Communication facilities are not staffed or 4) Communication facilities are not ready.
IRO-002-1	R2.	Each Reliability Coordinator shall determine the data requirements to support its reliability coordination tasks and shall request such data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities, or adjacent Reliability Coordinators.	The Reliability Coordinator demonstrated that it 1) determined its data requirements and requested that data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators with a material impact on the Bulk Electric System in its Reliability Coordination Area but did not request	The Reliability Coordinator demonstrated that it determined the majority but not all of its data requirements necessary to support its reliability coordination functions and requested that data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability	The Reliability Coordinator demonstrated that it determined 1) some but less than the majority of its data requirements necessary to support its reliability coordination functions and requested that data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent	The Reliability Coordinator failed to demonstrate that it 1) determined its data requirements necessary to support its reliability coordination functions and requested that data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators or 2) requested the data from three or more of its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners,

**Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the data from Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators with minimal impact on the Bulk Electric System in its Reliability Coordination Area or 2) determined its data requirements necessary to perform its reliability functions with the exceptions of data that may be needed for administrative purposes such as data reporting.	Coordinators.	Reliability Coordinators or 2) all of its data requirements necessary to support its reliability coordination functions but failed to demonstrate that it requested data from two of its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators.	Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators.
IRO-002-1	R3.	Each Reliability Coordinator – or its Transmission Operators and Balancing Authorities – shall provide, or arrange provisions for, data exchange to other	N/A	The Reliability Coordinator or designated Transmission	The Reliability Coordinator or designated Transmission	The Reliability Coordinator or designated Transmission

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Reliability Coordinators or Transmission Operators and Balancing Authorities via a secure network.		Operator and Balancing Authority has failed to demonstrate it provided or arranged provision for the exchange of data with one of the other Reliability Coordinators or Transmission Operators and Balancing Authorities.	Operator and Balancing Authority has failed to demonstrate it provided or arranged provision for the exchange of data with two of the other Reliability Coordinators or Transmission Operators and Balancing Authorities.	Operator and Balancing Authority has failed to demonstrate it provided or arranged provision for the exchange of data with three of the other Reliability Coordinators or Transmission Operators and Balancing Authorities.
IRO-002-1	R4.	Each Reliability Coordinator shall have multi-directional communications capabilities with its Transmission Operators and Balancing Authorities, and with neighboring Reliability Coordinators, for both voice and data exchange as required to meet reliability needs of the Interconnection.	N/A	The Reliability Coordinator has failed to demonstrate multi-directional communication capabilities to one of the Transmission Operators and Balancing Authorities in its Reliability Coordinator Area and with neighboring Reliability Coordinators.	The Reliability Coordinator has failed to demonstrate multi-directional communication capabilities to two or more of the Transmission Operators and Balancing Authorities in its Reliability Coordinator Area and with neighboring Reliability Coordinators.	The Reliability Coordinator has failed to demonstrate multi-directional communication capabilities to all of the Transmission Operators and Balancing Authorities in its Reliability Coordinator Area and with all neighboring Reliability Coordinators.
IRO-002-1	R5.	Each Reliability Coordinator shall have detailed real-time monitoring capability of its Reliability Coordinator Area and sufficient monitoring capability of its	The Reliability Coordinator's monitoring systems provide	The Reliability Coordinator has failed to demonstrate that is	The Reliability Coordinator has failed to demonstrate that is	The Reliability Coordinator has failed to demonstrate that is has detailed real-time

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		surrounding Reliability Coordinator Areas to ensure that potential or actual System Operating Limit or Interconnection Reliability Operating Limit violations are identified. Each Reliability Coordinator shall have monitoring systems that provide information that can be easily understood and interpreted by the Reliability Coordinator's operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant and highly reliable infrastructure.	information in a way that is not easily understood and interpreted by the Reliability Coordinator's operating personnel or particular emphasis was not given to alarm management and awareness systems, automated data transfers and synchronized information systems.	has detailed real-time monitoring capabilities in its Reliability Coordinator Area and sufficient monitoring capabilities of its surrounding Reliability Coordinator Areas to ensure that one potential or actual SOL or IROL violation is not identified.	has detailed real-time monitoring capabilities in its Reliability Coordinator Area and sufficient monitoring capabilities of its surrounding Reliability Coordinator Areas to ensure that two or more potential and actual SOL and IROL violations are not identified.	monitoring capabilities in its Reliability Coordinator Area and sufficient monitoring capabilities of its surrounding Reliability Coordinator Areas to ensure that all potential and actual SOL and IROL violations are identified.
IRO-002-1	R6.	Each Reliability Coordinator shall monitor Bulk Electric System elements (generators, transmission lines, buses, transformers, breakers, etc.) that could result in SOL or IROL violations within its Reliability Coordinator Area. Each Reliability Coordinator shall monitor both real and reactive power system flows, and operating reserves, and the status of Bulk Electric System elements that are or could be critical to SOLs and IROLs and system restoration requirements within its Reliability Coordinator Area.	The Reliability Coordinator failed to monitor: 1) the status, real power flow or reactive power flow of Bulk Electric System elements that could result in one SOL violations or 2) or operating reserves for a small portion of the Reliability Authority Area.	The Reliability Coordinator failed to monitor: 1) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing one IROL or to system restoration, 2) the status, real power flow or reactive power flow of Bulk Electric System elements that could result in multiple SOL violations, or	The Reliability Coordinator failed to monitor: 1) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing two or more IROLs; or one IROL and to system restoration, 2) the status, real power flow or reactive power flow of Bulk Electric System elements that could result in	The Reliability Coordinator failed to monitor: 1) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing all IROLs and to system restoration, or 2) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing all SOL violations and operating reserves.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) operating reserves.	multiple SOL violations and operating reserves, or 3) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing one IROL or system restoration and operating reserves.	
IRO-002-1	R7.	Each Reliability Coordinator shall have adequate analysis tools such as state estimation, pre- and post-contingency analysis capabilities (thermal, stability, and voltage), and wide-area overview displays.	The Reliability Coordinator failed to demonstrate that it has: 1) analysis tools capable of assessing all pre-contingency flows, 2) analysis tools capable of assessing all post-contingency flows, or 3) all necessary wide-area overview displays exist.	The Reliability Coordinator failed to demonstrate that it has: 1) analysis tools capable of assessing the majority of pre-contingency flows, 2) analysis tools capable of assessing the majority of post-contingency flows, or 3) the majority of necessary wide-area overview displays exist.	The Reliability Coordinator failed to demonstrate that it has: 1) analysis tools capable of assessing a minority of pre-contingency flows, 2) analysis tools capable of assessing a minority of post-contingency flows, or 3) a minority of necessary wide-area overview displays exist.	The Reliability Coordinator failed to demonstrate that it has: 1) analysis tools capable of assessing any pre-contingency flows, 2) analysis tools capable of assessing any post-contingency flows, or 3) any necessary wide-area overview displays exist.
IRO-002-1	R8.	Each Reliability Coordinator shall continuously monitor its Reliability Coordinator Area. Each Reliability	The Reliability Coordinator failed to demonstrate that:	The Reliability Coordinator failed to demonstrate that:	The Reliability Coordinator failed to demonstrate that:	The Reliability Coordinator failed to demonstrate that it

**Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Coordinator shall have provisions for backup facilities that shall be exercised if the main monitoring system is unavailable. Each Reliability Coordinator shall ensure SOL and IROL monitoring and derivations continue if the main monitoring system is unavailable.	1) it or a delegated entity monitored SOLs when the main monitoring system was unavailable or 2) it has provisions to monitor SOLs when the main monitoring system is not available.	1) it or a delegated entity monitored one IROL when the main monitoring system was unavailable or 2) it has provisions to monitor one IROL when the main monitoring system is not available.	1) it or a delegated entity monitored two or more IROLs when the main monitoring system was unavailable, 2) it or a delegated entity monitored SOLs and one IROL when the main monitoring system was unavailable 3) it has provisions to monitor two or more IROLs when the main monitoring system is not available, or 4) it has provisions to monitor SOLs and one IROL when the main monitoring system was unavailable.	continuously monitored its Reliability Authority Area.
IRO-002-1	R9.	Each Reliability Coordinator shall control its Reliability Coordinator analysis tools, including approvals for planned maintenance. Each Reliability Coordinator shall have procedures in place to mitigate the effects of analysis tool outages.	Reliability Coordinator has approval rights for planned maintenance outages of analysis tools but does not have approval rights for work on analysis tools that creates a greater	Reliability Coordinator has approval rights for planned maintenance but does not have plans to mitigate the effects of outages of the analysis tools.	Reliability Coordinator has approval rights for planned maintenance but does not have plans to mitigate the effects of outages of the analysis tools and does not have approval rights for	Reliability Coordinator approval is not required for planned maintenance.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			risk of an unplanned outage of the tools.		work on analysis tools that creates a greater risk of an unplanned outage of the tools.	
IRO-003-2	R1.	Each Reliability Coordinator shall monitor all Bulk Electric System facilities, which may include sub-transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.	N/A	N/A	The Reliability Coordinator failed to monitor all Bulk Electric System facilities, which may include sub-transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.	The Reliability Coordinator failed to monitor Bulk Electric System facilities, which may include sub-transmission information, within adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.
IRO-003-2	R2.	Each Reliability Coordinator shall know the current status of all critical	N/A	N/A	The Reliability Coordinator failed	The Reliability Coordinator failed to

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		facilities whose failure, degradation or disconnection could result in an SOL or IROL violation. Reliability Coordinators shall also know the status of any facilities that may be required to assist area restoration objectives.			to know either the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation or the status of any facilities that may be required to assist area restoration objectives.	know the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation and the status of any facilities that may be required to assist area restoration objectives.
IRO-004-1	R1.	Each Reliability Coordinator shall conduct next-day reliability analyses for its Reliability Coordinator Area to ensure that the Bulk Electric System can be operated reliably in anticipated normal and Contingency event conditions. The Reliability Coordinator shall conduct Contingency analysis studies to identify potential interface and other SOL and IROL violations, including overloaded transmission lines and transformers, voltage and stability limits, etc.	The Reliability Coordinator failed to conduct next-day reliability analyses or contingency analysis for its Reliability Coordinator Area for one (1) day during a calendar month.	The Reliability Coordinator failed to conduct next-day reliability analyses or contingency analysis for its Reliability Coordinator Area for two (2) to three (3) days during a calendar month.	The Reliability Coordinator failed to conduct next-day reliability analyses or contingency analysis for its Reliability Coordinator Area for four (4) to five (5) days during a calendar month.	The Reliability Coordinator failed to conduct next-day reliability analyses or contingency analysis for its Reliability Coordinator Area for more than five (5) days during a calendar month.
IRO-004-1	R2.	Each Reliability Coordinator shall pay particular attention to parallel flows to ensure one Reliability Coordinator Area does not place an unacceptable or undue Burden on an adjacent Reliability Coordinator Area.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor parallel flows to ensure one Reliability Coordinator Area does not place an unacceptable or undue Burden on an adjacent

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Reliability Coordinator Area.
IRO-004-1	R3.	Each Reliability Coordinator shall, in conjunction with its Transmission Operators and Balancing Authorities, develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs.	The Reliability Coordinator, in conjunction with its Transmission Operators and Balancing Authorities, failed to develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs for one (1) day during a calendar month.	The Reliability Coordinator, in conjunction with its Transmission Operators and Balancing Authorities, failed to develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs for two (2) to three (3) days during a calendar month.	The Reliability Coordinator, in conjunction with its Transmission Operators and Balancing Authorities, failed to develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs for four (4) to five (5) days during a calendar month.	The Reliability Coordinator, in conjunction with its Transmission Operators and Balancing Authorities, failed to develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs for more than five (5) days during a calendar month.
IRO-004-1	R4.	Each Transmission Operator, Balancing Authority, Transmission Owner, Generator Owner, Generator Operator, and Load-Serving Entity in the Reliability Coordinator Area shall provide information required for system studies, such as critical facility	The responsible entity in the Reliability Coordinator Area provided the information required for system	The responsible entity in the Reliability Coordinator Area provided the information required for system	The responsible entity in the Reliability Coordinator Area provided the information required for system	The responsible entity in the Reliability Coordinator Area provided the information required for system studies, such as critical facility

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		status, Load, generation, operating reserve projections, and known Interchange Transactions. This information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.	studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions, but said information was provided after the required time as stated in IRO-004-1 R4 for one (1) day during a calendar month.	studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions, but said information was provided after the required time as stated in IRO-004-1 R4 for two (2) to three (3) days during a calendar month.	studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions, but said information was provided after the required time as stated in IRO-004-1 R4 for four (4) to five (5) days during a calendar month.	status, Load, generation, operating reserve projections, and known Interchange Transactions, but said information was provided after the required time as stated in IRO-004-1 R4 for more than five (5) days during a calendar month.
IRO-004-1	R5.	Each Reliability Coordinator shall share the results of its system studies, when conditions warrant or upon request, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area. The Reliability Coordinator shall make study results available no later than 1500 Central Standard Time for the Eastern Interconnection and 1500 Pacific Standard Time for the Western Interconnection, unless circumstances warrant otherwise.	The Reliability Coordinator failed to share the results of its system studies, when conditions warranted or was requested, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area for one (1) day	The Reliability Coordinator failed to share the results of its system studies, when conditions warranted or was requested, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area for two (2) to three	The Reliability Coordinator failed to share the results of its system studies, when conditions warranted or was requested, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area for four (4) to five	The Reliability Coordinator failed to share the results of its system studies, when conditions warranted or was requested, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area for more than five (5) days during a calendar month.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			during a calendar month.	(3) days during a calendar month.	(5) days during a calendar month.	
IRO-004-1	R6.	If the results of these studies indicate potential SOL or IROL violations, the Reliability Coordinator shall direct its Transmission Operators, Balancing Authorities and Transmission Service Providers to take any necessary action the Reliability Coordinator deems appropriate to address the potential SOL or IROL violation.	The Reliability Coordinator failed to direct action to address a potential SOL or IROL violation on one (1) occasion during a calendar month.	The Reliability Coordinator failed to direct action to address a potential SOL or IROL violation on two (2) to three (3) occasions during a calendar month.	The Reliability Coordinator failed to direct action to address a potential SOL or IROL violation on four (4) to five (5) occasions during a calendar month.	The Reliability Coordinator failed to direct action to address a potential SOL or IROL violation on more than five (5) occasions during a calendar month.
IRO-004-1	R7.	Each Transmission Operator, Balancing Authority, and Transmission Service Provider shall comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events.	The responsible entity failed to comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events on one (1) occasion during a calendar month.	The responsible entity failed to comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events on two (2) to three (3) occasions during a calendar month.	The responsible entity failed to comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events on four (4) to five (5) occasions during a calendar month.	The responsible entity failed to comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events on more than five (5) occasions during a calendar month.
IRO-005-2	R1.	Each Reliability Coordinator shall monitor its Reliability Coordinator Area parameters, including but not limited to the following:	The Reliability Coordinator failed to monitor one (1) of the elements listed in IRO-005-2 R1.1 through R1.10.	The Reliability Coordinator failed to monitor two (2) of the elements listed in IRO-005-2 R1.1 through R1.10.	The Reliability Coordinator failed to monitor three (3) of the elements listed in IRO-005-2 R1.1 through R1.10.	The Reliability Coordinator failed to monitor more than three (3) of the elements listed in IRO-005-2 R1.1 through R1.10.
IRO-005-2	R1.1.	Current status of Bulk Electric System elements (transmission or generation	N/A	N/A	N/A	The Reliability Coordinator failed to

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		including critical auxiliaries such as Automatic Voltage Regulators and Special Protection Systems) and system loading.				monitor the current status of Bulk Electric System elements (transmission or generation including critical auxiliaries such as Automatic Voltage Regulators and Special Protection Systems) and system loading.
IRO-005-2	R1.2.	Current pre-contingency element conditions (voltage, thermal, or stability), including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor current pre-contingency element conditions (voltage, thermal, or stability); including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.
IRO-005-2	R1.3.	Current post-contingency element conditions (voltage, thermal, or stability), including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor current post-contingency element conditions (voltage, thermal, or stability); including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.
IRO-005-2	R1.4.	System real and reactive reserves	N/A	N/A	N/A	The Reliability

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(actual versus required).				Coordinator failed to monitor system real and reactive reserves (actual versus required).
IRO-005-2	R1.5.	Capacity and energy adequacy conditions.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor capacity and energy adequacy conditions.
IRO-005-2	R1.6.	Current ACE for all its Balancing Authorities.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor current ACE for all its Balancing Authorities.
IRO-005-2	R1.7.	Current local or Transmission Loading Relief procedures in effect.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor current local or Transmission Loading Relief procedures in effect.
IRO-005-2	R1.8.	Planned generation dispatches.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor planned generation dispatches.
IRO-005-2	R1.9.	Planned transmission or generation outages.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor planned transmission or generation outages.
IRO-005-2	R1.10.	Contingency events.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor contingency events.
IRO-005-2	R2.	Each Reliability Coordinator shall be aware of all Interchange Transactions	N/A	N/A	The Reliability Coordinator was	The Reliability Coordinator failed to

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		that wheel through, source, or sink in its Reliability Coordinator Area, and make that Interchange Transaction information available to all Reliability Coordinators in the Interconnection.			aware of all Interchange Transactions that wheeled through, sourced or sunked in its Reliability Coordinator Area, but failed to make that Interchange Transaction information available to all Reliability Coordinators in the Interconnection.	be aware of all Interchange Transactions that wheeled through, sourced or sunked in its Reliability Coordinator Area, and failed to make that Interchange Transaction information available to all Reliability Coordinators in the Interconnection.
IRO-005-2	R3.	As portions of the transmission system approach or exceed SOLs or IROLs, the Reliability Coordinator shall work with its Transmission Operators and Balancing Authorities to evaluate and assess any additional Interchange Schedules that would violate those limits. If a potential or actual IROL violation cannot be avoided through proactive intervention, the Reliability Coordinator shall initiate control actions or emergency procedures to relieve the violation without delay, and no longer than 30 minutes. The Reliability Coordinator shall ensure all resources, including load shedding, are available to address a potential or actual IROL violation.	N/A	The Reliability Coordinator worked with its Transmission Operators and Balancing Authorities, as portions of the transmission system approached or exceeded SOLs or IROLs, to evaluate and assess any additional Interchange Schedules that would violate those limits and initiated control actions or emergency procedures to	The Reliability Coordinator worked with its Transmission Operators and Balancing Authorities, as portions of the transmission system approached or exceeded SOLs or IROLs, to evaluate and assess any additional Interchange Schedules that would violate those limits and ensured all resources, including load shedding, were	The Reliability Coordinator failed to work with its Transmission Operators and Balancing Authorities, as portions of the transmission system approached or exceeded SOLs or IROLs, to evaluate and assess any additional Interchange Schedules that would violate those limits and failed to initiate control actions or emergency procedures to relieve the violation within 30 minutes.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				relieve the violation within 30 minutes, but failed to ensure all resources, including load shedding, were available to address a potential or actual IROL violation.	available to address a potential or actual IROL violation, but failed to initiate control actions or emergency procedures to relieve the violation within 30 minutes.	
IRO-005-2	R4.	Each Reliability Coordinator shall monitor its Balancing Authorities' parameters to ensure that the required amount of operating reserves is provided and available as required to meet the Control Performance Standard and Disturbance Control Standard requirements. If necessary, the Reliability Coordinator shall direct the Balancing Authorities in the Reliability Coordinator Area to arrange for assistance from neighboring Balancing Authorities. The Reliability Coordinator shall issue Energy Emergency Alerts as needed and at the request of its Balancing Authorities and Load-Serving Entities.	N/A	The Reliability Coordinator failed to direct the Balancing Authorities in the Reliability Coordinator Area to arrange for assistance from neighboring Balancing Authorities.	The Reliability Coordinator failed to issue Energy Emergency Alerts as needed and at the request of its Balancing Authorities and Load-Serving Entities.	The Reliability Coordinator failed to monitor its Balancing Authorities' parameters to ensure that the required amount of operating reserves was provided and available as required to meet the Control Performance Standard and Disturbance Control Standard requirements.
IRO-005-2	R5.	Each Reliability Coordinator shall identify the cause of any potential or actual SOL or IROL violations. The Reliability Coordinator shall initiate the control action or emergency procedure to relieve the potential or actual IROL violation without delay, and no longer than 30 minutes. The Reliability Coordinator shall be able to utilize all resources, including load	N/A	N/A	The Reliability Coordinator identified the cause of a potential or actual SOL or IROL violation, but failed to initiate a control action or emergency procedure to relieve	The Reliability Coordinator failed to identify the cause of a potential or actual SOL or IROL violation and failed to initiate a control action or emergency procedure to relieve the potential or actual

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shedding, to address an IROL violation.			the potential or actual IROL violation within 30 minutes.	IROL violation.
IRO-005-2	R6.	Each Reliability Coordinator shall ensure its Transmission Operators and Balancing Authorities are aware of Geo-Magnetic Disturbance (GMD) forecast information and assist as needed in the development of any required response plans.	N/A	N/A	The Reliability Coordinator ensured its Transmission Operators and Balancing Authorities were aware of Geo-Magnetic Disturbance (GMD) forecast information, but failed to assist, when needed, in the development of any required response plans.	The Reliability Coordinator failed to ensure its Transmission Operators and Balancing Authorities were aware of Geo-Magnetic Disturbance (GMD) forecast information.
IRO-005-2	R7.	The Reliability Coordinator shall disseminate information within its Reliability Coordinator Area, as required.	N/A	N/A	N/A	The Reliability Coordinator failed to disseminate information within its Reliability Coordinator Area, when required.
IRO-005-2	R8.	Each Reliability Coordinator shall monitor system frequency and its Balancing Authorities' performance and direct any necessary rebalancing to return to CPS and DCS compliance. The Transmission Operators and Balancing Authorities shall utilize all resources, including firm load	N/A	N/A	The Reliability Coordinator monitored system frequency and its Balancing Authorities' performance but failed to direct any	The Reliability Coordinator failed to monitor system frequency and its Balancing Authorities' performance and direct any necessary rebalancing to return

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shedding, as directed by its Reliability Coordinator to relieve the emergent condition.			necessary rebalancing to return to CPS and DCS compliance.	to CPS and DCS compliance or the responsible entity failed to utilize all resources, including firm load shedding, as directed by its Reliability Coordinator to relieve the emergent condition.
IRO-005-2	R9.	The Reliability Coordinator shall coordinate with Transmission Operators, Balancing Authorities, and Generator Operators as needed to develop and implement action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations. The Reliability Coordinator shall coordinate pending generation and transmission maintenance outages with Transmission Operators, Balancing Authorities, and Generator Operators as needed in both the real-time and next-day reliability analysis timeframes.	N/A	The Reliability Coordinator coordinated with Transmission Operators, Balancing Authorities, and Generator Operators, as needed, to develop action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations but failed to implement said plans, or the Reliability Coordinator coordinated pending generation and transmission maintenance outages with Transmission	The Reliability Coordinator failed to coordinate with Transmission Operators, Balancing Authorities, and Generator Operators as needed to develop and implement action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations, or the Reliability Coordinator failed to coordinate pending generation and transmission maintenance outages with Transmission Operators,	The Reliability Coordinator failed to coordinate with Transmission Operators, Balancing Authorities, and Generator Operators as needed to develop and implement action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations and the Reliability Coordinator failed to coordinate pending generation and transmission maintenance outages with Transmission Operators, Balancing Authorities, and Generator Operators as needed in both the real-time and next-day

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Operators, Balancing Authorities, and Generator Operators as needed in the real-time reliability analysis timeframe but failed to coordinate pending generation and transmission maintenance outages in the next-day reliability analysis timeframe.	Balancing Authorities, and Generator Operators as needed in both the real-time and next-day reliability analysis timeframes.	reliability analysis timeframes.
IRO-005-2	R10.	As necessary, the Reliability Coordinator shall assist the Balancing Authorities in its Reliability Coordinator Area in arranging for assistance from neighboring Reliability Coordinator Areas or Balancing Authorities.	N/A	N/A	N/A	The Reliability Coordinator failed to assist the Balancing Authorities in its Reliability Coordinator Area in arranging for assistance from neighboring Reliability Coordinator Areas or Balancing Authorities, when necessary.
IRO-005-2	R11.	The Reliability Coordinator shall identify sources of large Area Control Errors that may be contributing to Frequency Error, Time Error, or Inadvertent Interchange and shall discuss corrective actions with the appropriate Balancing Authority. The	N/A	The Reliability Coordinator identified sources of large Area Control Errors that were contributing to Frequency Error,	The Reliability Coordinator identified sources of large Area Control Errors that were contributing to Frequency Error,	The Reliability Coordinator failed to identify sources of large Area Control Errors that were contributing to Frequency Error,

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Reliability Coordinator shall direct its Balancing Authority to comply with CPS and DCS.		Time Error, or Inadvertent Interchange and discussed corrective actions with the appropriate Balancing Authority but failed to direct the Balancing Authority to comply with CPS and DCS.	Time Error, or Inadvertent Interchange but failed to discuss corrective actions with the appropriate Balancing Authority.	Time Error, or Inadvertent Interchange.
IRO-005-2	R12.	Whenever a Special Protection System that may have an inter-Balancing Authority, or inter-Transmission Operator impact (e.g., could potentially affect transmission flows resulting in a SOL or IROL violation) is armed, the Reliability Coordinators shall be aware of the impact of the operation of that Special Protection System on inter-area flows. The Transmission Operator shall immediately inform the Reliability Coordinator of the status of the Special Protection System including any degradation or potential failure to operate as expected.	N/A	N/A	N/A	The Reliability Coordinator failed to be aware of the impact on inter-area flows of an inter-Balancing Authority or inter-Transmission Operator, following the operation of a Special Protection System that is armed (e.g., could potentially affect transmission flows resulting in a SOL or IROL violation), or the Transmission Operator failed to immediately inform the Reliability Coordinator of the status of the Special

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Protection System including any degradation or potential failure to operate as expected.
IRO-005-2	R13.	Each Reliability Coordinator shall ensure that all Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities operate to prevent the likelihood that a disturbance, action, or non-action in its Reliability Coordinator Area will result in a SOL or IROL violation in another area of the Interconnection. In instances where there is a difference in derived limits, the Reliability Coordinator and its Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall always operate the Bulk Electric System to the most limiting parameter.	N/A	N/A	N/A	The Reliability Coordinator failed to shall ensure that all Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities operated to prevent the likelihood that a disturbance, action, or non-action in its Reliability Coordinator Area could result in a SOL or IROL violation in another area of the Interconnection or the responsible entity failed to operate the Bulk Electric System to the most limiting parameter in instances where there was a difference in derived limits..
IRO-005-2	R14.	Each Reliability Coordinator shall make known to Transmission Service	N/A	N/A	N/A	The Reliability Coordinator failed to

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Providers within its Reliability Coordinator Area, SOLs or IROLs within its wide-area view. The Transmission Service Providers shall respect these SOLs or IROLs in accordance with filed tariffs and regional Total Transfer Calculation and Available Transfer Calculation processes.				make known to Transmission Service Providers within its Reliability Coordinator Area, SOLs or IROLs within its wide-area view, or the Transmission Service Providers failed to respect these SOLs or IROLs in accordance with filed tariffs and regional Total Transfer Calculation and Available Transfer Calculation processes.
IRO-005-2	R15.	Each Reliability Coordinator who foresees a transmission problem (such as an SOL or IROL violation, loss of reactive reserves, etc.) within its Reliability Coordinator Area shall issue an alert to all impacted Transmission Operators and Balancing Authorities in its Reliability Coordinator Area without delay. The receiving Reliability Coordinator shall disseminate this information to its impacted Transmission Operators and Balancing Authorities. The Reliability Coordinator shall notify all impacted Transmission Operators, Balancing Authorities, when the transmission problem has been mitigated.	N/A	The Reliability Coordinator failed to notify all impacted Transmission Operators, Balancing Authorities, when the transmission problem had been mitigated.	N/A	The Reliability Coordinator who foresaw a transmission problem (such as an SOL or IROL violation, loss of reactive reserves, etc.) within its Reliability Coordinator Area failed to issue an alert to all impacted Transmission Operators and Balancing Authorities in its Reliability Coordinator Area, or the receiving Reliability

**Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Coordinator failed to disseminate this information to its impacted Transmission Operators and Balancing Authorities.
IRO-005-2	R16.	Each Reliability Coordinator shall confirm reliability assessment results and determine the effects within its own and adjacent Reliability Coordinator Areas. The Reliability Coordinator shall discuss options to mitigate potential or actual SOL or IROL violations and take actions as necessary to always act in the best interests of the Interconnection at all times.	N/A	N/A	The Reliability Coordinator confirmed the reliability assessment results and determine the effects within its own and adjacent Reliability Coordinator Areas and discussed options to mitigate potential or actual SOL or IROL violations, but failed to take actions as necessary to always act in the best interests of the Interconnection at all times.	The Reliability Coordinator failed to confirm reliability assessment results and determine the effects within its own and adjacent Reliability Coordinator Areas, or failed to discuss options to mitigate potential or actual SOL or IROL violations and take actions as necessary to always act in the best interests of the Interconnection at all times.
IRO-005-2	R17.	When an IROL or SOL is exceeded, the Reliability Coordinator shall evaluate the local and wide-area impacts, both real-time and post-contingency, and determine if the actions being taken are appropriate and sufficient to return the system to within	N/A	N/A	N/A	The Reliability Coordinator either failed to evaluate the local and wide-area impacts of an IROL or SOL that was exceeded, in either

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>IROL in thirty minutes. If the actions being taken are not appropriate or sufficient, the Reliability Coordinator shall direct the Transmission Operator, Balancing Authority, Generator Operator, or Load-Serving Entity to return the system to within IROL or SOL.</p>				<p>real-time or post-contingency, or the Reliability Coordinator evaluated the local and wide-area impacts of an IROL or SOL that was exceeded, both real-time and post-contingency, and determined that the actions being taken were not appropriate and sufficient to return the system to within IROL in thirty (30) minutes, but failed to direct the Transmission Operator, Balancing Authority, Generator Operator, or Load-Serving Entity to return the system to within IROL or SOL.</p>
IRO-006-4	R1.	<p>A Reliability Coordinator experiencing a potential or actual SOL or IROL violation within its Reliability Coordinator Area shall, with its authority and at its discretion, select one or more procedures to provide transmission loading relief. These procedures can be a “local” (regional, interregional, or sub-regional)</p>	<p>For each TLR in the Eastern Interconnection, the Reliability Coordinator violates one (1) requirement of the applicable Interconnection-wide procedure</p>	<p>For each TLR in the Eastern Interconnection, the Reliability Coordinator violated two (2) to three (3) requirements of the applicable Interconnection-</p>	<p>For each TLR in the Eastern Interconnection, the applicable Reliability Coordinator violated four (4) to five (5) requirements of the applicable</p>	<p>For each TLR in the Eastern Interconnection, the Reliability Coordinator violated six (6) or more of the requirements of the applicable Interconnection-wide procedure.</p>

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		transmission loading relief procedure or one of the following Interconnection-wide procedures:		wide procedure	Interconnection-wide procedure	
IRO-006-4	R1.1	The Interconnection-wide Transmission Loading Relief (TLR) procedure for use in the Eastern Interconnection provided in Attachment 1-IRO-006-4. The TLR procedure alone is an inappropriate and ineffective tool to mitigate an IROL violation due to the time required to implement the procedure. Other acceptable and more effective procedures to mitigate actual IROL violations include: reconfiguration, redispatch, or load shedding.				While attempting to mitigate an existing IROL violation in the Eastern Interconnection, the Reliability Coordinator applied TLR as the sole remedy for an existing IROL violation.
IRO-006-4	R1.2	The Interconnection-wide transmission loading relief procedure for use in the Western Interconnection is WECC-IRO-STD-006-0 provided at: ftp://www.nerc.com/pub/sys/all_up dl/standards/rrs/IRO-STD-006-0_17Jan07.pdf .				While attempting to mitigate an existing constraint in the Western Interconnection using the “WSCC Unscheduled Flow Mitigation Plan”, the Reliability Coordinator did not follow the procedure correctly.
IRO-006-4	R1.3	The Interconnection-wide transmission loading relief procedure for use in ERCOT is				While attempting to mitigate an existing constraint in

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		provided as Section 7 of the ERCOT Protocols, posted at: http://www.ercot.com/mktrules/protocols/current.html				ERCOT using Section 7 of the ERCOT Protocols, the Reliability Coordinator did not follow the procedure correctly.
IRO-006-4	R2	The Reliability Coordinator shall only use local transmission loading relief or congestion management procedures to which the Transmission Operator experiencing the potential or actual SOL or IROL violation is a party.	N/A	N/A	N/A	A Reliability Coordinator implemented local transmission loading relief or congestion management procedures to relieve congestion but the Transmission Operator experiencing the congestion was not a party to those procedure
IRO-006-4	R3	Each Reliability Coordinator with a relief obligation from an Interconnection-wide procedure shall follow the curtailments as directed by the Interconnection-wide procedure. A Reliability Coordinator desiring to use a local procedure as a substitute for curtailments as directed by the Interconnection-wide procedure shall obtain prior approval of the local procedure from the ERO.	N/A	N/A	N/A	A Reliability Coordinator implemented local transmission loading relief or congestion management procedures as a substitute for curtailment as directed by the Interconnection-wide procedure but

**Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the local procedure had not received prior approval from the ERO
IRO-006-4	R4	When Interconnection-wide procedures are implemented to curtail Interchange Transactions that cross an Interconnection boundary, each Reliability Coordinator shall comply with the provisions of the Interconnection-wide procedure.	When requested to curtail an Interchange Transaction that crosses an Interconnection boundary utilizing an Interconnection-wide procedure, the responding Reliability Coordinator did not comply with the provisions of the Interconnection-wide procedure as requested by the initiating Reliability Coordinator	N/A	N/A	N/A
IRO-006-4	R5	During the implementation of relief procedures, and up to the point that emergency action is necessary, Reliability Coordinators and Balancing Authorities shall comply with applicable Interchange scheduling standards.	The Reliability Coordinators or Balancing Authorities did not comply with applicable Interchange	N/A	N/A	N/A

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			scheduling standards during the implementation of the relief procedures, up to the point emergency action is necessary			
IRO-014-1	R1.	The Reliability Coordinator shall have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability. These Operating Procedures, Processes, or Plans shall address Scenarios that affect other Reliability Coordinator Areas as well as those developed in coordination with other Reliability Coordinators.	N/A	N/A	The Reliability Coordinator has Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability, but failed to address Scenarios that affect other Reliability Coordinator Areas.	The Reliability Coordinator failed to have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability.
IRO-014-1	R1.1.	These Operating Procedures, Processes, or Plans shall collectively address, as a minimum, the following:	The Reliability Coordinator failed to include one of	The Reliability Coordinator failed to include two of	The Reliability Coordinator failed to include more	N/A

**Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in there Operating Procedures, Processes, or Plans.	the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in there Operating Procedures, Processes, or Plans.	than two of the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in there Operating Procedures, Processes, or Plans.	
IRO-014-1	R1.1.1.	Communications and notifications, including the conditions under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators.	N/A	N/A	N/A	The Reliability Coordinator failed to address communications and notifications, including the conditions under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.2.	Energy and capacity shortages.	N/A	N/A	N/A	The Reliability Coordinator failed to address energy and capacity shortages in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.3.	Planned or unplanned outage information.	N/A	N/A	N/A	The Reliability Coordinator failed to

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						address planned or unplanned outage information in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.4.	Voltage control, including the coordination of reactive resources for voltage control.	N/A	N/A	N/A	The Reliability Coordinator failed to address voltage control, including the coordination of reactive resources for voltage control in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.5.	Coordination of information exchange to support reliability assessments.	N/A	N/A	N/A	The Reliability Coordinator failed to address the coordination of information exchange to support reliability assessments in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.6.	Authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas.	N/A	N/A	N/A	The Reliability Coordinator failed to address authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas in its Operating Procedure, Process or Plan.
IRO-014-1	R2.	Each Reliability Coordinator's	N/A	N/A	N/A	The Reliability

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operating Procedure, Process, or Plan that requires one or more other Reliability Coordinators to take action (e.g., make notifications, exchange information, or coordinate actions) shall be:				Coordinator's Operating Procedure, Process, or Plan failed to comply with either IRO-014-1 R2.1 or R2.2.
IRO-014-1	R2.1.	Agreed to by all the Reliability Coordinators required to take the indicated action(s).	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan was not agreed to by all the Reliability Coordinators required to take the indicated action(s).
IRO-014-1	R2.2.	Distributed to all Reliability Coordinators that are required to take the indicated action(s).	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan was not distributed to all Reliability Coordinators that are required to take the indicated action(s).
IRO-014-1	R3.	A Reliability Coordinator's Operating Procedures, Processes, or Plans developed to support a Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan shall include:	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to comply with either IRO-014-1 R3.1 or R3.2.
IRO-014-1	R3.1.	A reference to the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to reference the

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.
IRO-014-1	R3.2.	The agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to include the agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.
IRO-014-1	R4.	Each of the Operating Procedures, Processes, and Plans addressed in Reliability Standard IRO-014 Requirement 1 and Requirement 3 shall:	N/A	N/A	N/A	The Reliability Coordinator developed an Operating Procedure, Process, or Plan in accordance with IRO-014 Requirement 1 and Requirement 3, but failed to comply with one of the elements listed in IRO-014-1 R4.1 through R4.3.
IRO-014-1	R4.1.	Include version control number or date	N/A	N/A	N/A	The Reliability Operator failed to include the version control number or date in its Operating

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Procedure, Process, or Plan.
IRO-014-1	R4.2.	Include a distribution list.	N/A	N/A	N/A	The Reliability Operator failed to include a distribution list in its Operating Procedure, Process, or Plan.
IRO-014-1	R4.3.	Be reviewed, at least once every three years, and updated if needed.	N/A	N/A	N/A	The Reliability Operator failed to review, at least once every three years, and update if needed, its Operating Procedure, Process, or Plan.
IRO-015-1	R1.	The Reliability Coordinator shall follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators.	N/A	The Reliability Coordinator failed to follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators but no adverse reliability impacts resulted from the incident.	N/A	The Reliability Coordinator failed to follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators and adverse reliability impacts resulted from the incident.
IRO-015-1	R1.1.	The Reliability Coordinator shall make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator	N/A	The Reliability Coordinator failed to make notifications to other Reliability	N/A	The Reliability Coordinator failed to make notifications to other Reliability Coordinators of

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Areas.		Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas but no adverse reliability impacts resulted from the incident.		conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas and adverse reliability impacts resulted from the incident.
IRO-015-1	R2.	The Reliability Coordinator shall participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.	N/A	N/A	N/A	The Reliability Coordinator failed to participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.
IRO-015-1	R2.1.	The frequency of these conference calls shall be agreed upon by all involved Reliability Coordinators and shall be at least weekly.	N/A	N/A	N/A	The Reliability Operator failed to participate in the assessment of the need and frequency of conference calls with other Reliability Operators.
IRO-015-1	R3.	The Reliability Coordinator shall provide reliability-related information as requested by other Reliability Coordinators.	N/A	N/A	N/A	The Reliability Coordinator failed to provide reliability-related information as requested by other Reliability Coordinators.
IRO-016-1	R1.	The Reliability Coordinator that	The Reliability	N/A	N/A	The Reliability

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.</p>	<p>Coordinator that identified a potential, expected, or actual problem that required the actions of one or more other Reliability Coordinators, contacted the other Reliability Coordinator(s) to confirm that there was a problem, discussed options and decided upon a solution to prevent or resolve the identified problem, but failed to have evidence that it coordinated with other Reliability Coordinators.</p>			<p>Coordinator that identified a potential, expected, or actual problem that required the actions of one or more other Reliability Coordinators failed to contact the other Reliability Coordinator(s) to confirm that there was a problem, discuss options and decide upon a solution to prevent or resolve the identified problem.</p>
IRO-016-1	R1.1.	<p>If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.</p>	<p>The responsible entity agreed on the problem and the actions to take to prevent or mitigate the system condition, implemented the agreed-upon solution, but failed to notify the involved Reliability</p>	N/A	N/A	<p>The responsible entity agreed on the problem and the actions to take to prevent or mitigate the system condition, but failed to implement the agreed-upon solution.</p>

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Coordinators of the action(s) taken.			
IRO-016-1	R1.2.	If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).	N/A	N/A	N/A	The involved Reliability Coordinators could not agree on the problem(s), but a Reliability Coordinator failed to re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
IRO-016-1	R1.2.1.	If time permits, this re-evaluation shall be done before taking corrective actions.	N/A	N/A	N/A	The Reliability Coordinator failed to re-evaluate the problem prior to taking corrective actions, during periods when time was not an issue.
IRO-016-1	R1.2.2.	If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.	N/A	N/A	N/A	The Reliability Coordinator failed to operate as though the problem(s) exist(s) until the conflicting system status was resolved, during periods when time was an issue.
IRO-016-1	R1.3.	If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.	N/A	N/A	N/A	The Reliability Coordinator implemented a solution other than the most conservative solution, when

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						agreement on the solution could not be reached.
IRO-016-1	R2.	The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.	N/A	N/A	N/A	The Reliability Coordinator failed to document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

**Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-006-0.1	R1.	Each Transmission Service Provider shall document its procedure on the use of Capacity Benefit Margin (CBM) (scheduling of energy against a CBM reservation). The procedure shall include the following three components:	The Transmission Service Provider documented its procedure on the use of Capacity Benefit Margin (CBM) but failed to include one (1) of the components as specified in R1.1, R1.2 or R1.3.	The Transmission Service Provider documented its procedure on the use of Capacity Benefit Margin (CBM) but failed to include two (2) of the components as specified in R1.1, R1.2 or R1.3.	The Transmission Service Provider documented its procedure on the use of Capacity Benefit Margin (CBM) but failed to include three (3) of the components as specified in R1.1, R1.2 or R1.3.	The Transmission Service Provider failed to document its procedure on the use of Capacity Benefit Margin (CBM).
MOD-006-0.1	R1.1.	Require that CBM be used only after the following steps have been taken (as time permits): all non-firm sales have been terminated, Direct-Control Load Management has been implemented, and customer interruptible demands have been interrupted. CBM may be used to reestablish Operating Reserves.	N/A	The Transmission Service Provider required that CBM be used only after all non-firm sales have been terminated and Direct-Control Load Management has been implemented but failed to include customer interruptible demands that have been interrupted.	The Transmission Service Provider required that CBM be used only after all non-firm sales have been terminated but failed to include Direct-Control Load Management has been implemented and customer interruptible demands that have been interrupted.	The Transmission Service Provider failed to require that CBM be used only after all non-firm sales have been terminated, Direct-Control Load Management has been implemented and customer interruptible demands that have been interrupted.
MOD-006-0.1	R1.2.	Require that CBM shall only be used if the Load-Serving Entity calling for its use is experiencing a generation deficiency and its Transmission Service Provider is also experiencing Transmission Constraints relative to imports of energy on its transmission	N/A	The Transmission Service Provider required that CBM shall only be used if the Load-Serving Entity calling for its use is	N/A	The Transmission Service Provider failed to require that CBM shall only be used if the Load-Serving Entity calling for

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		system.		experiencing a generation deficiency but failed to require that CBM shall only be used if its Transmission Service Provider is also experiencing Transmission Constraints relative to imports of energy on its transmission system.		its use is experiencing a generation deficiency and its Transmission Service Provider is also experiencing Transmission Constraints relative to imports of energy on its transmission system.
MOD-006-0.1	R1.3.	Describe the conditions under which CBM may be available as Non-Firm Transmission Service.	N/A	N/A	N/A	The Transmission Service Provider has failed to describe the conditions under which CBM may be available as Non-Firm Transmission Service.
MOD-006-0.1	R2.	Each Transmission Service Provider shall make its CBM use procedure available on a web site accessible by the Regional Reliability Organizations, NERC, and transmission users.	The Transmission Service Provider has demonstrated the procedure is available on the Web but is deficient with minor details.	N/A	N/A	The Transmission Service Provider has failed to provide the procedure on the Web as directed by the requirement.
MOD-007-0	R1.	Each Transmission Service Provider that uses CBM shall report (to the Regional Reliability Organization,	N/A	Each Transmission Service Provider that uses CBM	N/A	Each Transmission Service Provider that uses CBM

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		NERC and the transmission users) the use of CBM by the Load-Serving Entities' Loads on its system, except for CBM sales as Non-Firm Transmission Service. (This use of CBM shall be consistent with the Transmission Service Provider's procedure for use of CBM.)		reported (to the Regional Reliability Organization, NERC and the transmission users) the use of CBM by the Load-Serving Entities' Loads on its system but failed to use CBM that is consistent with the Transmission Service Provider's procedure for use of CBM.		failed to report (to the Regional Reliability Organization, NERC and the transmission users) the use of CBM by the Load-Serving Entities' Loads on its system.
MOD-007-0	R2.	The Transmission Service Provider shall post the following three items within 15 calendar days after the use of CBM for an Energy Emergency. This posting shall be on a web site accessible by the Regional Reliability Organizations, NERC, and transmission users.	The Transmission Service Provider that uses CBM for an Energy Emergency complied with the posting of the 3 required items but is deficient regarding minor details.	The Transmission Service Provider that uses CBM for an Energy Emergency complied with the posting but is deficient regarding one of the 3 requirements.	The Transmission Service Provider that uses CBM for an Energy Emergency complied with the posting but is deficient regarding two of the 3 requirements.	The Transmission Service Provider that uses CBM for an Energy Emergency did not comply with the posting as required.
MOD-007-0	R2.1.	Circumstances.	The Transmission Service Provider posted the circumstance more than 15 but less than or equal to 20 calendar days after the use of CBM for	The Transmission Service Provider posted the circumstance more than 20 but less than or equal to 25 calendar days after the use of CBM for	The Transmission Service Provider posted the circumstance more than 25 but less than or equal to 30 calendar days after the use of CBM for	The Transmission Service Provider failed to post the circumstance more than 30 calendar days after the use of CBM for an Energy Emergency.

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			an Energy Emergency.	an Energy Emergency.	an Energy Emergency.	
MOD-007-0	R2.2.	Duration.	The Transmission Service Provider posted the duration more than 15 but less than or equal to 20 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider posted the duration more than 20 but less than or equal to 25 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider posted the duration more than 25 but less than or equal to 30 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider failed to post the duration more than 30 calendar days after the use of CBM for an Energy Emergency.
MOD-007-0	R2.3.	Amount of CBM used.	The Transmission Service Provider posted the amount of CBM used more than 15 but less than or equal to 20 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider posted the amount of CBM used more than 20 but less than or equal to 25 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider posted the amount of CBM used more than 25 but less than or equal to 30 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider failed to post the amount of CBM used more than 30 calendar days after the use of CBM for an Energy Emergency.
MOD-010-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the appropriate equipment characteristics, system data, and existing and future Interchange	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than or equal to 50% of the appropriate equipment characteristics, system data, and existing and future	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than or equal to 75% of the appropriate equipment characteristics, system data, and existing and future	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R 1	Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.
MOD-010-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide this steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. If no schedule exists, then these entities shall provide the data on request (30 calendar days).	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than or equal to 50% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than or equal to 75% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>OR</p> <p>If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 30 but less than or equal to 35 calendar days following the request.</p>	<p>OR</p> <p>If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 35 but less than or equal to 40 calendar days following the request.</p>	<p>OR</p> <p>If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 40 but less than or equal to 45 calendar days following the request.</p>	<p>If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide data more than 45 calendar days following the request.</p>
MOD-012-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R1) shall provide appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than 50% of the appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than 75% of the appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1	simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.
MOD-012-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R4) shall provide dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. If no schedule exists, then these entities shall provide data on request (30 calendar days).	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1 OR	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than 50% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than 75% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR If no schedule

**Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 30 but less than or equal to 35 calendar days following the request.	If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 35 but less than or equal to 40 calendar days following the request.	If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 40 but less than or equal to 45 calendar days following the request.	exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide data more than 45 calendar days following the request.
MOD-016-1.1	R1.	The Planning Authority and Regional Reliability Organization shall have documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses.	N/A	The Planning Authority and Regional Reliability Organization has documentation identifying the scope and details of the actual and forecast data but failed to have documentation identifying the scope data and details for one (1) of the following actual and forecast data to be reported for system modeling and reliability analyses: (a) Demand data,	The Planning Authority and Regional Reliability Organization has documentation identifying the scope and details of the actual and forecast data but failed to have documentation identifying the scope data and details for two (2) of the following actual and forecast data to be reported for system modeling and reliability analyses: (a) Demand data,	The Planning Authority and Regional Reliability Organization has failed to have documentation identifying the scope and details of the actual and forecast data to be reported for system modeling and reliability analyses.

**Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(b) Net Energy for Load data, or (c) controllable DSM data.	(b) Net Energy for Load data, or (c) controllable DSM data.	
MOD-016-1.1	R1.1.	<p>The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021.</p> <p>The data submittal requirements shall stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.</p>	<p>The Planning Authority and Regional Reliability Organization failed to ensure that consistent data is supplied for less than or equal to 25% or the Reliability Standards as specified in R1.1</p>	<p>The Planning Authority and Regional Reliability Organization failed to ensure that consistent data is supplied for greater than 25% but less than or equal to 50% of the Reliability Standards as specified in R1.1.</p>	<p>The Planning Authority and Regional Reliability Organization failed to ensure that consistent data is supplied for greater than 50% but less than or equal to 75% of the Reliability Standards as specified in R1.1.</p>	<p>The Planning Authority and Regional Reliability Organization failed to ensure that consistent data is supplied for greater than 75% of the Reliability Standards as specified in R1.1.</p> <p>OR</p> <p>The Planning Authority and Regional Reliability Organization failed to stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.</p>

**Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-016-1.1	R2.	The Regional Reliability Organization shall distribute its documentation required in Requirement 1 and any changes to that documentation, to all Planning Authorities that work within its Region.	N/A	N/A	The Regional Reliability Organization distributed its documentation as specified in R1 but failed to distribute any changes to that documentation, to all Planning Authorities that work within its Region.	The Regional Reliability Organization failed to distribute its documentation as specified in R1 to all Planning Authorities that work within its Region.
MOD-016-1.1	R2.1.	The Regional Reliability Organization shall make this distribution within 30 calendar days of approval.	The Regional Reliability Organization distributed the documentation more than 30 but less than or equal to 37 calendar days following approval.	The Regional Reliability Organization made the distribution more than 37 but less than or equal to 51 calendar days following approval.	The Regional Reliability Organization made the distribution more than 51 but less than or equal to 58 calendar days following approval.	The Regional Reliability Organization failed to make the distribution more than 58 calendar days following approval.
MOD-016-1.1	R3.	The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area.	N/A	N/A	The Planning Authority distributed its documentation as specified in R1 for reporting customer data but failed to distribute any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work	The Planning Authority failed to distribute its documentation as specified in R1 for reporting customer data to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area.

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					within its Planning Authority Area.	
MOD-016-1.1	R3.1.	The Planning Authority shall make this distribution within 30 calendar days of approval.	The Planning Authority distributed the documentation more than 30 but less than or equal to 37 calendar days following approval.	The Planning Authority made the distribution more than 37 but less than or equal to 51 calendar days following approval.	The Planning Authority made the distribution more than 51 but less than or equal to 58 calendar days following approval.	The Planning Authority failed to make the distribution more than 58 calendar days following approval
MOD-017-0.1	R1.	The Load-Serving Entity, Planning Authority, and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R 1.	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide one of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide two of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide three of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide all of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.
MOD-017-0.1	R1.1.	Integrated hourly demands in megawatts (MW) for the prior year.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide Integrated hourly demands in megawatts (MW) for the prior year on an annual basis.
MOD-017-0.1	R1.2.	Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the prior year.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, and Resource Planner

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						failed to provide monthly and annual peak hour actual demands in MW Net Energy for Load in gigawatthours (GWh) for the prior year.
MOD-017-0.1	R1.3.	Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years.
MOD-017-0.1	R1.4.	Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested.

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-018-0	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or dispersed basis) shall:	N/A	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to report one (1) of the items as specified in R1.1, R1.2, or R1.3.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to report two (2) of the items as specified in R1.1, R1.2, or R1.3.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to report all of the items as specified in R1.1, R1.2, and R1.3.
MOD-018-0	R1.1.	Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included.
MOD-018-0	R1.2.	Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to address assumptions, methods, and the manner in which uncertainties are

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						treated in the forecasts of aggregated peak demands and Net Energy for Load.
MOD-018-0	R1.3.	Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to address items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) as described in the reporting procedures developed for Standard MOD-016-1_R 1.
MOD-018-0	R2.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days).	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization,	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization,	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization,	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to report the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization,

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Load-Serving Entity, Planning Authority, and Resource Planner more than 30 but less than or equal to 45 calendar days following the request.	Load-Serving Entity, Planning Authority, and Resource Planner more than 45 but less than or equal to 60 calendar days following the request.	Load-Serving Entity, Planning Authority, and Resource Planner more than 60 but less than or equal to 75 calendar days following the request.	Load-Serving Entity, Planning Authority, and Resource Planner more than 75 calendar days following the request.
MOD-019-0.1	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R 1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually less than or equal to 25% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 25% but less than or equal to 50% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 50% but less than or equal to 75% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 75% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R 1.	Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R1.	Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R1.	(Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R1.
MOD-020-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 30 but less than 45 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 45 but less than 60 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 60 but less than 75 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to make known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 75 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.
MOD-021-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource	Load-Serving Entity,	Load-Serving Entity,	Load-Serving Entity,	Load-Serving Entity,

**Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed.	Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how one (1) of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how two (2) of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how three (3) of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	Transmission Planner, and Resource Planner's forecasts failed to document how the Demand and energy effects of DSM programs are addressed.
MOD-021-0	R2.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R 1.	N/A	N/A	N/A	The Load-Serving Entity, Transmission Planner, and Resource Planner failed to include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0 R 1.
MOD-021-0	R3.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days).	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 30 but less than 45 calendar days following the request from NERC.	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 45 but less than 60 calendar days following the request from NERC.	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 60 but less than 75 calendar days following the request from NERC.	The Load-Serving Entity, Transmission Planner, and Resource Planner failed to provide documentation on the treatment of its DSM programs more than 75 calendar days following the request from NERC.

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
NUC-001-1	R1.	The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt.	The Nuclear Plant Generator Operator did not verify receipt of the proposed NPIR's.	The Nuclear Plant Generator Operator submitted an incomplete proposed NPIR to the applicable transmission entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to some applicable entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to any applicable entities.
NUC-001-1	R2.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.	N/A	N/A	N/A	The Nuclear Plant Generator Operator or the applicable Transmission Entity does not have in effect one or more agreements that include NPIRs and document the implementation of the NPIRs.
NUC-001-1	R3.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall	The applicable Transmission Entity incorporated the NPIRs into its planning analyses and identified no areas of concern but it did not	The applicable Transmission Entity incorporated the NPIRs into its planning analyses and identified one or more areas of concern but did not	The applicable Transmission Entity did not incorporate the NPIRs into its planning analyses of the electric system.	N/A

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		communicate the results of these analyses to the Nuclear Plant Generator Operator.	communicate these results to the Nuclear Plant Generator Operator.	communicate these results to the Nuclear Plant Generator Operator.		
NUC-001-1	R4.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall:	The applicable Transmission Entity failed to incorporate one or more applicable NPIRs into their operating analyses.	The applicable Transmission Entity failed to incorporate any NPIRs into their operating analyses OR did not inform NPG operator when their ability of assess the operation of the electric system affecting the NPIRs was lost.	The applicable Transmission Entity failed to operate the system to meet the NPIRs	N/A
NUC-001-1	R4.1	Incorporate the NPIRs into their operating analyses of the electric system.	N/A	N/A	N/A	N/A
NUC-001-1	R4.2	Operate the electric system to meet the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-1	R4.3	Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.	N/A	N/A	N/A	N/A
NUC-001-1	R5.	The Nuclear Plant Generator Operator shall operate per the Agreements developed in	The Nuclear Operator failed to operate the plant in accordance with one	The Nuclear Operator failed to operate the plant in accordance with one	The Nuclear Operator failed to operate the plant in accordance with	N/A

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		accordance with this standard.	or more of the administrative or training elements within the agreements.	or two of the technical, operations, and maintenance or communication elements within the agreements.	three or more of the technical, operations, and maintenance or communication elements within the agreements.	
NUC-001-1	R6.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs.	The Nuclear Operator or Transmission Entity failed to coordinate outages or maintenance activities in accordance with one or more of the <u>administrative</u> elements within the agreements.	The Nuclear Operator or Transmission Entity failed to provide outage or maintenance <u>schedules</u> to the appropriate parties as described in the agreement or on a time period consistent with the agreements.	The Nuclear Operator or Transmission Entity failed to coordinate one or more outages or maintenance activities in accordance the requirements of the agreements.	N/A
NUC-001-1	R7.	Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of <u>proposed</u> changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of <u>actual</u> changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that <u>may</u> impact the	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of <u>actual</u> changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that <u>directly</u> impact the	N/A

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		electric system to meet the NPIRs.	ability of the electric system to meet the NPIRs.	ability of the electric system to meet the NPIRs.	ability of the electric system to meet the NPIRs.	
NUC-001-1	R8.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of <u>proposed</u> changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of <u>actual</u> changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that <u>may</u> impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of <u>actual</u> changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that <u>directly impacts</u> the ability of the electric system to meet the NPIRs.	N/A
NUC-001-1	R9.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2:	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing one or more sub-components of R9.1.	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing from one to five of the combined sub-components in R9.2, R9.3 and R9.4.	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing from six to ten of the combined sub-components in R9.2, R9.3 and R9.4.	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing eleven or more of the combined sub-components in R9.2, R9.3 and R9.4.
NUC-001-1	R9.1	Administrative elements:				

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
NUC-001-1	R9.1.1	Definitions of key terms used in the agreement.				
NUC-001-1	R9.1.2	Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.				
NUC-001-1	R9.1.3	A requirement to review the agreement(s) at least every three years.				
NUC-001-1	R9.1.4	A dispute resolution mechanism.				
NUC-001-1	R9.2	Technical requirements and analysis:				
NUC-001-1	R9.2.1	Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.				
NUC-001-1	R9.2.2	Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.				
NUC-001-1	R9.2.3	Types of planning and operational analyses performed specifically to support the NPIRs,				

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		including the frequency of studies and types of Contingencies and scenarios required.				
NUC-001-1	R9.3	Operations and maintenance coordination:				
NUC-001-1	R9.3.1	Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.				
NUC-001-1	R9.3.2	Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.				
NUC-001-1	R9.3.3	Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.				
NUC-001-1	R9.3.4	Provisions to address mitigating actions needed				

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.				
NUC-001-1	R9.3.5	Provision to consider nuclear plant coping times required by the NPLRs and their relation to the coordination of grid and nuclear plant restoration following a nuclear plant loss of Off-site Power.				
NUC-001-1	R9.3.6	Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.				
NUC-001-1	R9.3.7	Coordination of the NPIRs with transmission				

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		system Special Protection Systems and underfrequency and undervoltage load shedding programs.				
NUC-001-1	R9.4	Communications and training:				
NUC-001-1	R9.4.1	Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.				
NUC-001-1	R9.4.2	Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.				
NUC-001-1	R9.4.3	Provisions for coordinating investigations of causes				

**Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.				
NUC-001-1	R9.4.4	Provisions for supplying information necessary to report to government agencies, as related to NPIRs.				
NUC-001-1	R9.4.5	Provisions for personnel training, as related to NPIRs.				

**Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PER-001-0	R1.	Each Transmission Operator and Balancing Authority shall provide operating personnel with the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.	N/A	N/A	The Transmission Operator and Balancing Authority has failed to demonstrate the communication to the operating personnel their responsibility OR their authority to implement real-time actions to ensure a stable and reliable operation of the Bulk Electric System.	The Transmission Operator and Balancing Authority has failed to demonstrate the communication to the operating personnel their responsibility AND authority to implement real-time actions to ensure a stable and reliable operation of the Bulk Electric System.
PER-002-0	R1.	Each Transmission Operator and Balancing Authority shall be staffed with adequately trained operating personnel.	The applicable entity did not adequately staff and train operating personnel, affecting 5% or less of its operating personnel.	The applicable entity did not adequately staff and train operating personnel, affecting between 5-10% of its operating personnel.	The applicable entity did not adequately staff and train operating personnel, affecting 10-15%, inclusive, of its operating personnel.	The applicable entity did not adequately staff and train operating personnel, affecting greater than 15% of its operating personnel.
PER-002-0	R2.	Each Transmission Operator and Balancing Authority shall have a training program for all operating personnel that are in:	Each Transmission Operator and Balancing Authority has produced the training program for more than 75% but less than 100% of their real-time operating personnel.	Each Transmission Operator and Balancing Authority has produced the training program for more than 50% but less than or equal to 75% of their real-time operating personnel.	Each Transmission Operator and Balancing Authority has produced the training program for more than 25% but less than or equal to 50% of their real-time operating personnel.	Each Transmission Operator and Balancing Authority has produced the training program for more than or equal to 0% but less than or equal to 25% of their real-time operating personnel.
PER-002-0	R2.1.	Positions that have the primary responsibility, either directly or through	N/A	N/A	N/A	The Transmission Operator and Balancing Authority

**Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		communications with others, for the real-time operation of the interconnected Bulk Electric System.				failed to produce training program for their operating personnel.
PER-002-0	R2.2.	Positions directly responsible for complying with NERC standards.	N/A	N/A	N/A	The Transmission Operator and Balancing Authority failed to produce training program for positions directly responsible for complying with NERC Standards.
PER-002-0	R3.	For personnel identified in Requirement R2, the Transmission Operator and Balancing Authority shall provide a training program meeting the following criteria:	The applicable entity did not comply with one of the four required elements.	The applicable entity did not comply with two of the four required elements.	The applicable entity did not comply with three of the four required elements.	The applicable entity did not comply with any of the four required elements.
PER-002-0	R3.1.	A set of training program objectives must be defined, based on NERC and Regional Reliability Organization standards, entity operating procedures, and applicable regulatory requirements. These objectives shall reference the knowledge and competencies needed to apply those standards, procedures, and requirements to normal,	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for less than 25% of the applicable BA and TOP NERC and Regional Reliability Organizations standards, entity	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 25% or more but less than 50% of the applicable BA & TOP NERC and Regional Reliability Organizations	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 50% or more but less than 75% of the applicable BA & TOP NERC and Regional Reliability Organizations	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 75% or more of the applicable BA & TOP NERC and Regional Reliability Organizations standards, entity

Complete Violation Severity Level Matrix (PER) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		emergency, and restoration conditions for the Transmission Operator and Balancing Authority operating positions.	operating procedures, and regulatory requirements.)	standards, entity operating procedures, and regulatory requirements.)	standards, entity operating procedures, and regulatory requirements.)	operating procedures, and regulatory requirements.)
PER-002-0	R3.2.	The training program must include a plan for the initial and continuing training of Transmission Operator and Balancing Authority operating personnel. That plan shall address knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. OR The responsible entity does not have a plan for initial training of operating personnel. OR The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. OR The responsible entity does not have a plan for initial training of operating personnel. AND The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. AND The responsible entity does not have a plan for initial training of operating personnel. OR The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. AND The responsible entity does not have a plan for initial training of operating personnel. AND The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.
PER-002-0	R3.3.	The training program must include training time for all Transmission Operator and Balancing Authority operating personnel to ensure their operating proficiency.	The responsible entity has produced the training program with more than 75% but less than 100% of operating personnel provided with training time.	The responsible entity has produced the training program with more than 50% but less than or equal to 75% of operating personnel provided with training time.	The responsible entity has produced the training program with more than 25% but less than or equal to 50% of operating personnel provided with training time.	The responsible entity has produced the training program with more than or equal to 0% but less than or equal to 25% of operating personnel provided with training time.
PER-002-0	R3.4.	Training staff must be identified, and the staff must be competent in both knowledge of system operations and instructional capabilities.	N/A	The responsible entity has produced the training program with training staff identified that lacks knowledge of system	The responsible entity has produced the training program with training staff identified that lacks knowledge of system	The responsible entity has produced the training program with no training staff identified.

**Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				operations. OR The responsible entity has produced the training program with training staff identified that lacks instructional capabilities.	operations. AND The responsible entity has produced the training program with training staff identified that lacks instructional capabilities.	
PER-002-0	R4.	For personnel identified in Requirement R2, each Transmission Operator and Balancing Authority shall provide its operating personnel at least five days per year of training and drills using realistic simulations of system emergencies, in addition to other training required to maintain qualified operating personnel.	The applicable entity did not provide five days per year of training and drills, as directed by the requirement, affecting 5% or less of its operating personnel.	The applicable entity did not provide five days per year of training and drills, as directed by the requirement, affecting between 5-10% of its operating personnel.	The applicable entity did not provide five days per year of training and drills, as directed by the requirement, affecting 10-15%, inclusive, of its operating personnel.	The applicable entity did not provide five days per year of training and drills, as directed by the requirement, affecting greater than 15% of its operating personnel.
PER-003-0	R1.	Each Transmission Operator, Balancing Authority, and Reliability Coordinator shall staff all operating positions that meet both of the following criteria with personnel that are NERC-certified for the applicable functions:	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 0 hours and less than 12 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 12 hours and less than 36 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 36 hours and less than 72 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 72 hours for any operating position for a calendar month.
PER-003-0	R1.1.	Positions that have the primary responsibility,	The responsible entity failed to staff an	The responsible entity failed to staff an	The responsible entity failed to staff an	The responsible entity failed to staff an

**Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		either directly or through communications with others, for the real-time operation of the interconnected Bulk Electric System.	operating position with NERC certified personnel for greater than 0 hours and less than 12 hours for any operating position for a calendar month.	operating position with NERC certified personnel for greater than 12 hours and less than 36 hours for any operating position for a calendar month.	operating position with NERC certified personnel for greater than 36 hours and less than 72 hours for any operating position for a calendar month.	operating position with NERC certified personnel for greater than 72 hours for any operating position for a calendar month.
PER-003-0	R1.2.	Positions directly responsible for complying with NERC standards.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 0 hours and less than 12 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 12 hours and less than 36 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 36 hours and less than 72 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 72 hours for any operating position for a calendar month.
PER-004-1	R1.	Each Reliability Coordinator shall be staffed with adequately trained and NERC-certified Reliability Coordinator operators, 24 hours per day, seven days per week.	N/A	N/A	N/A	The responsible entity has failed to be staffed with adequately trained and NERC-certified Reliability Coordinator operators, 24 hours per day, seven days per week.
PER-004-1	R2.	All Reliability Coordinator operating personnel shall each complete a minimum of five days per year of training and drills using realistic simulations of system emergencies, in addition to other training required to maintain qualified operating personnel.	The Reliability Coordinator's operating personnel completed at least 4 (but less than 5) days of emergency training.	The Reliability Coordinator's operating personnel completed at least 3 (but less than 4) days of emergency training.	The Reliability Coordinator's operating personnel completed at least 2 (but less than 3) days of emergency training.	The Reliability Coordinator's operating personnel completed less than 2 days of emergency training.
PER-004-1	R3.	Reliability Coordinator	Reliability	Reliability	Reliability	Reliability

**Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		operating personnel shall have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	Coordinator personnel have a comprehensive understanding of the interactions with at least 75% and less than 100% of neighboring Reliability Coordinator areas.	Coordinator personnel have a comprehensive understanding of the interactions with 50% or more and less than 75% of neighboring Reliability Coordinator areas.	Coordinator personnel have a comprehensive understanding of the interactions with 25% or more and less than 50% of neighboring Reliability Coordinator areas.	Coordinator personnel have a comprehensive understanding of the interactions less than 25% of neighboring Reliability Coordinator areas.
PER-004-1	R4.	Reliability Coordinator operating personnel shall have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.	Reliability Coordinator operating personnel have an extensive understanding of the operations of more than 75% and less than 100% of all Balancing Authorities, Transmission Operators and Generator Operators in the Reliability Coordinator Area.	Reliability Coordinator operating personnel have an extensive understanding of the operations of more than 50% and less than 75% of all Balancing Authorities, Transmission Operators and Generator Operators in the Reliability Coordinator Area.	Reliability Coordinator operating personnel have an extensive understanding of the operations of more than 25% and less than 50% of all Balancing Authorities, Transmission Operators and Generator Operators in the Reliability Coordinator Area.	Reliability Coordinator operating personnel have an extensive understanding of the operations of less than 25% of all Balancing Authorities, Transmission Operators and Generator Operators in the Reliability Coordinator Area.
PER-004-1	R5.	Reliability Coordinator operating personnel shall place particular attention on SOLs and IROLs and inter-tie facility limits. The Reliability Coordinator shall ensure protocols are in place to allow Reliability Coordinator operating personnel to have the best available information at all times.	Reliability Coordinator has failed to provide its operating personnel with less than 25% of the SOL and IROL limits and for inter-tie facility limits OR the protocols to ensure best available data at all times is not in	Reliability Coordinator has failed to provide its operating personnel with 25% or more and less than 50% of the SOL and IROL limits and for inter-tie facility limits.	Reliability Coordinator has failed to provide its operating personnel with 50% or more and less than 75% of the SOL and IROL limits and for inter-tie facility limits.	Reliability Coordinator has failed to provide its operating personnel with 75% or more of the SOL and IROL limits and for inter-tie facility limits.

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			place.			

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-001-1	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.	N/A	N/A	The responsible entity was familiar with the purpose of protection system schemes applied in its area but failed to be familiar with the limitations of protection system schemes applied in its area.	The responsible entity failed to be familiar with the purpose and limitations of protection system schemes applied in its area.
PRC-001-1	R2.	Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:	N/A	N/A	N/A	The responsible entity failed to notify any reliability entity of relay or equipment failures.
PRC-001-1	R2.1.	If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.	N/A	Notification of relay or equipment failure was not made to the Transmission Operator and Host Balancing Authority, but corrective action was taken.	Notification of relay or equipment failure was made to the Transmission Operator and Host Balancing Authority, but corrective action was not taken.	Notification of relay or equipment failure was not made to the Transmission Operator and Host Balancing Authority, and corrective action was not taken.
PRC-001-1	R2.2.	If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.	N/A	Notification of relay or equipment failure was not made to the Reliability Coordinator and affected Transmission Operators and Balancing	Notification of relay or equipment failure was made to the Reliability Coordinator and affected Transmission Operators and Balancing	Notification of relay or equipment failure was not made to the Reliability Coordinator and affected Transmission Operators and Balancing

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Authorities, but corrective action was taken.	Authorities, but corrective action was not taken.	Authorities, and corrective action was not taken.
PRC-001-1	R3.	A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.	N/A	N/A	N/A	N/A
PRC-001-1	R3.1.	Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.	The Generator Operator failed to coordinate one new protective system or one protective system change with either its Transmission Operator or its Host Balancing Authority or both.	The Generator Operator failed to coordinate two new protective systems or two protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Generator Operator failed to coordinate three new protective systems or three protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Generator Operator failed to coordinate more than three new protective systems or more than three changes with its Transmission Operator and Host Balancing Authority.
PRC-001-1	R3.2.	Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.	The Transmission Operator failed to coordinate one new protective system or one protective system change with either its Transmission Operator or its Host Balancing Authority or both.	The Transmission Operator failed to coordinate two new protective systems or two protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Transmission Operator failed to coordinate three new protective systems or three protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Transmission Operator failed to coordinate more than three new protective systems or more than three system changes with neighboring Transmission Operators and Balancing Authorities.
PRC-001-1	R4.	Each Transmission Operator shall coordinate protection systems on major transmission lines and interconnections with neighboring Generator Operators,	The Transmission Operator failed to coordinate protection systems on major	The Transmission Operator failed to coordinate protection systems on major	The Transmission Operator failed to coordinate protection systems on major	The Transmission Operator failed to coordinate protection systems on major

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Operators, and Balancing Authorities.	transmission lines and interconnections with one of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	transmission lines and interconnections with two of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	transmission lines and interconnections with three of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	transmission lines and interconnections with three or more of its neighboring Generator Operators, Transmission Operators, and Balancing Authorities.
PRC-001-1	R5.	A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the protection systems of others:	N/A	N/A	N/A	The responsible entity failed to coordinate changes in generation, transmission, load or operating conditions that could require changes in the protection systems of others:
PRC-001-1	R5.1.	Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.	N/A	N/A	N/A	The Generator Operator failed to notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.
PRC-001-1	R5.2.	Each Transmission Operator shall notify neighboring Transmission	N/A	N/A	N/A	The Transmission Operator failed to

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems.				notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems.
PRC-001-1	R6.	Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.	N/A	N/A	Notification of a change in status of a Special Protection System was not made to the affected Transmission Operators and Balancing Authorities.	The responsible entity failed to monitor the status of each Special Protection System in its area, and did not notify affected Transmission Operators and Balancing Authorities of each change in status.
PRC-004-1	R1.	The Transmission Owner and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Reliability Organization's	Documentation of Misoperations is complete, but documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and there are no associated Corrective Action Plans.	Misoperations have not been analyzed

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		procedures developed for Reliability Standard PRC-003 Requirement 1.				
PRC-004-1	R2.	The Generator Owner shall analyze its generator Protection System Misoperations, and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	Documentation of Misoperations is complete, but documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and there are no associated Corrective Action Plans.	Misoperations have not been analyzed
PRC-004-1	R3.	The Transmission Owner, any Distribution Provider that owns a transmission Protection System, and the Generator Owner shall each provide to its Regional Reliability Organization, documentation of its Misoperations analyses and Corrective Action Plans according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses and its Corrective Action Plans, but did not provide these according to the Regional Reliability Organization's procedures.	N/A	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses but did not provide its Corrective Action Plans.	The responsible entity did not provide its Regional Reliability Organization with documentation of its Misoperations analyses and did not provide its Corrective Action Plans.
PRC-005-1	R1.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the	N/A	N/A	The responsible entity that owned a transmission Protection System or Generator Owner that owned a generation Protection System failed to have either	The responsible entity that owned a transmission Protection System or Generator Owner that owned a generation Protection System failed to have a

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reliability of the BES. The program shall include:			a Protection System maintenance program or a Protection System testing program for Protection Systems that affect the reliability of the BES.	Protection System maintenance program and a Protection System testing program for Protection Systems that affect the reliability of the BES.
PRC-005-1	R1.1.	Maintenance and testing intervals and their basis.	Maintenance and testing intervals and their basis was missing for no more than 25% of the applicable devices.	Maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the applicable devices.	Maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the applicable devices.	Maintenance and testing intervals and their basis was missing for more than 75% but of the applicable devices.
PRC-005-1	R1.2.	Summary of maintenance and testing procedures.	Summary of maintenance and testing procedures was missing for no more than 25% of the applicable devices.	Summary of maintenance and testing procedures was missing for more than 25% but less than or equal to 50% of the applicable devices.	Summary of maintenance and testing procedures was missing for more than 50% but less than or equal to 75% of the applicable devices.	Summary of maintenance and testing procedures was missing for more than 75% but of the applicable devices.
PRC-005-1	R2.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on	The responsible entity provided documentation of its Protection System maintenance and testing program for more than 30 but less than or equal to 40 days following a request from its Regional Reliability	The responsible entity provided documentation of its Protection System maintenance and testing program for more than 40 but less than or equal to 50 days following a request from its Regional Reliability	The responsible entity provided documentation of its Protection System maintenance and testing program for more than 50 but less than or equal to 60 days following a request from its Regional Reliability	The responsible entity did not provide documentation of its Protection System maintenance and testing program for more than 60 days following a request from its Regional Reliability

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		request (within 30 calendar days). The documentation of the program implementation shall include:	Organization and/or NERC.	Organization and/or NERC.	Organization and/or NERC.	Organization and/or NERC.
PRC-005-1	R2.1.	Evidence Protection System devices were maintained and tested within the defined intervals.	Evidence Protection System devices were maintained and tested within the defined intervals was missing for no more than 25% of the applicable devices.	Evidence Protection System devices were maintained and tested within the defined intervals was missing more than 25% but less than or equal to 50% of the applicable devices.	Evidence Protection System devices were maintained and tested within the defined intervals was missing more than 50% but less than or equal to 75% of the applicable devices.	Evidence Protection System devices were maintained and tested within the defined intervals was missing more than 75% of the applicable devices.
PRC-005-1	R2.2.	Date each Protection System device was last tested/maintained.	Date each Protection System device was last tested/maintained was missing no more than 25% of the applicable devices.	Date each Protection System device was last tested/maintained was missing for more than 25% but less than or equal to 50% of the applicable devices.	Date each Protection System device was last tested/maintained was missing for more than 50% but less than or equal to 75% of the applicable devices.	Date each Protection System device was last tested/maintained was missing for more than 75% of the applicable devices.
PRC-007-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall ensure that its UFLS program is consistent with its Regional Reliability Organization's UFLS program requirements.	The evaluation of the entity's UFLS program for consistency with its Regional Reliability Organization's UFLS program is incomplete or inconsistent in one or more of the Regional Reliability Organization program	The amount of load shedding is less than 95 percent of the Regional requirement in any of the load steps.	The amount of load shedding is less than 90 percent of the Regional requirement in any of the load steps.	The amount of load shedding is less than 85 percent of the Regional requirement in any of the load steps.

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			requirements, but is consistent with the required amount of load shedding.			
PRC-007-0	R2.	The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database.	The responsible entity has demonstrated the reporting of information but failed to satisfy one database reporting requirements.	The responsible entity has demonstrated the reporting of information but failed to satisfy two database reporting requirements.	The responsible entity has demonstrated the reporting of information but failed to satisfy at three database reporting requirements.	The responsible entity has demonstrated the reporting of information but failed to satisfy four or more database reporting requirements or has not provided the information.
PRC-007-0	R3.	The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days).	The responsible entity has provided the documentation in more than 30 calendar days but less than 40 calendar days.	The responsible entity has provided the documentation in more than 39 calendar days but less than 50 calendar days.	The responsible entity has provided the documentation in more than 49 calendar days but less than 60 calendar days.	The responsible entity has not provided the documentation within 60 calendar days.
PRC-008-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification,	The UFLS equipment identification, schedule for UFLS equipment testing or the schedule for UFLS equipment testing in the responsible entity's UFLS equipment	The UFLS equipment identification, schedule for UFLS equipment testing or the schedule for UFLS equipment testing in the responsible entity's UFLS equipment	The UFLS equipment identification, schedule for UFLS equipment testing or the schedule for UFLS equipment testing in the responsible entity's UFLS equipment	The UFLS equipment identification, schedule for UFLS equipment testing or the schedule for UFLS equipment testing in the responsible entity's UFLS equipment

Complete Violation Severity Level Matrix (PRC) Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.	maintenance and testing program was missing for no more than 25% of the applicable relays.	maintenance and testing program was missing for more than 25% but less than or equal to 50% of the applicable relays.	maintenance and testing program was missing for more than 50% but less than or equal to 75% of the applicable relays.	maintenance and testing program was missing for more than 75% of the applicable relays.
PRC-008-0	R2.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its UFLS equipment maintenance and testing program for more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its UFLS equipment maintenance and testing program for more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its UFLS equipment maintenance and testing program for more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its UFLS equipment maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-009-0	R1.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions	The responsible entity that owns or operates a UFLS program failed to include one of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events	The responsible entity that owns or operates a UFLS program failed to include two of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events	The responsible entity that owns or operates a UFLS program failed to include three of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events	The responsible entity that owns or operates a UFLS program failed to conduct an analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:	resulting in system frequency excursions below the initializing set points of the UFLS program.	resulting in system frequency excursions below the initializing set points of the UFLS program.	resulting in system frequency excursions below the initializing set points of the UFLS program.	points of the UFLS program.
PRC-009-0	R1.1.	A description of the event including initiating conditions.	N/A	N/A	N/A	The responsible entity failed to include a description of the event, including initiating conditions, that triggered an analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R1.2.	A review of the UFLS set points and tripping times.	N/A	N/A	N/A	The responsible entity failed to include a review of the UFLS set points and tripping times in the analysis of the performance of UFLS equipment and Program

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R1.3.	A simulation of the event.	N/A	N/A	N/A	The responsible entity failed to conduct a simulation of the event that triggered an analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R1.4.	A summary of the findings.	N/A	N/A	N/A	The responsible entity failed to include a summary of the findings in the analysis of the performance of UFLS equipment

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R2.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.	The responsible entity has provided the documentation in more than 90 calendar days but less than 105 calendar days.	The responsible entity has provided the documentation in more than 105 calendar days but less than 129 calendar days.	The responsible entity has provided the documentation in more than 129 calendar days but less than 145 calendar days.	The responsible entity has provided the documentation in 145 calendar days or more.
PRC-010-0	R1.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and	The responsible entity conducted an assessment of the effectiveness of its UVLS system within 5 years or as required by changes in system conditions but did not include the associated Transmission Planner(s) and Planning	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 5 years but did in less than or equal to 7 years.	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 7 years but did in less than or equal to 10 years.	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 10 years.

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Planning Authority(ies).	Authority(ies).			
PRC-010-0	R1.1.	This assessment shall include, but is not limited to:	N/A	The assessment of the effectiveness of the responsible entity's UVLS system did not address one of the elements in R1.1.1 through R1.1.3.	The assessment of the effectiveness of the responsible entity's UVLS system did not address two of the elements in R1.1.1 through R1.1.3.	The assessment of the effectiveness of the responsible entity's UVLS system did not address any of the elements in R1.1.1 through R1.1.3.
PRC-010-0	R1.1.1.	Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.	The responsible entity is non-compliant in the coordination of the UVLS programs with no more than 25% of the appropriate protection and control systems in the Region and with other Regional Reliability Organizations.	The responsible entity is non-compliant in the coordination of the UVLS programs with more than 25% but less than or equal to 50% of the appropriate protection and control systems in the Region and with other Regional Reliability Organizations.	The responsible entity is non-compliant in the coordination of the UVLS programs with more than 50% but less than or equal to 75% of the appropriate protection and control systems in the Region and with other Regional Reliability Organizations.	The responsible entity is non-compliant in the coordination of the UVLS programs with more than 75% of the appropriate protection and control systems in the Region and with other Regional Reliability Organizations.
PRC-010-0	R1.1.2.	Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.	The responsible entity's analysis was non-compliant in that no more than 25% of the simulations needed to demonstrate consistency with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-	The responsible entity's analysis was non-compliant in that more than 25% but less than or equal to 50% of the simulations needed to demonstrate consistency with Reliability Standards TPL-001-0, TPL-002-0, TPL-	The responsible entity's analysis was non-compliant in that more than 50% but less than or equal to 75% of the simulations needed to demonstrate consistency with Reliability Standards TPL-001-0, TPL-002-0, TPL-	The responsible entity's analysis was non-compliant in that more than 75% of the simulations needed to demonstrate consistency with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			0 were not performed.	003-0 and TPL-004-0 were not performed.	003-0 and TPL-004-0 were not performed.	0 were not performed.
PRC-010-0	R1.1.3.	A review of the voltage set points and timing.	The responsible entity's analysis is non-compliant in that a review of no more than 25% of the corresponding voltage set points and timing was not performed.	The responsible entity's analysis is non-compliant in that a review of more than 25% but less than or equal to 50% of the corresponding voltage set points and timing was not performed.	The responsible entity's analysis is non-compliant in that a review of more than 50% but less than 75% of the corresponding voltage set points and timing was not performed.	The responsible entity's analysis is non-compliant in that a review of more than 75% of the corresponding voltage set points and timing was not performed.
PRC-010-0	R2.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).	The responsible entity provided documentation of its current UVLS program assessment more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its current UVLS program assessment more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its current UVLS program assessment more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its current UVLS program assessment for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-011-0	R1.	The Transmission Owner and Distribution Provider that owns a UVLS system shall have a UVLS equipment maintenance and testing program in place. This program shall include:	The responsible entity's UVLS equipment maintenance and testing program did not address one of the elements in R1.1 through R1.6.	The responsible entity's UVLS equipment maintenance and testing program did not address two or three of the elements in R1.1 through R1.6.	The responsible entity's UVLS equipment maintenance and testing program did not address four or five of the elements in R1.1 through R1.6.	The responsible entity's UVLS equipment maintenance and testing program did not address any of the elements in R1.1 through R1.6.
PRC-011-0	R1.1.	The UVLS system identification	The responsible	The responsible	The responsible	The responsible

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		which shall include but is not limited to:	entity's UVLS program system identification did not address one of the elements in R1.1.1 through R1.1.4.	entity's UVLS program system identification did not address two of the elements in R1.1.1 through R1.1.4.	entity's UVLS program system identification did not address three of the elements in R1.1.1 through R1.1.4.	entity's UVLS program system identification did not address any of the elements in R1.1.1 through R1.1.4.
PRC-011-0	R1.1.1.	Relays.	The responsible entity's UVLS program system identification was missing no more than 25% of the applicable relays.	The responsible entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the applicable relays.	The responsible entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the applicable relays.	The responsible entity's UVLS program system identification was missing more than 75% of the applicable relays.
PRC-011-0	R1.1.2.	Instrument transformers.	The responsible entity's UVLS program system identification was missing no more than 25% of the applicable instrument transformers.	The responsible entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the applicable instrument transformers.	The responsible entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the applicable instrument transformers.	The responsible entity's UVLS program system identification was missing more than 75% of the applicable instrument transformers.
PRC-011-0	R1.1.3.	Communications systems, where appropriate.	The responsible entity's UVLS program system identification was missing no more than 25% of the appropriate communication systems.	The responsible entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the appropriate communication systems.	The responsible entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the appropriate communication systems.	The responsible entity's UVLS program system identification was missing more than 75% of the appropriate communication systems.
PRC-011-0	R1.1.4.	Batteries.	The responsible	The responsible	The responsible	The responsible

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			entity's UVLS program system identification was missing no more than 25% of the applicable batteries.	entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the applicable batteries.	entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the applicable batteries.	entity's UVLS program system identification was missing more than 75% of the applicable batteries.
PRC-011-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for no more than 25% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 75% of the UVLS equipment.
PRC-011-0	R1.3.	Summary of testing procedure.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for no more than 25% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 25% but less than or equal to 50% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 50% but less than or equal to 75% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 75% of the UVLS equipment.

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-011-0	R1.4.	Schedule for system testing.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for no more than 25% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 25% but less than or equal to 50% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 50% but less than or equal to 75% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 75% of the UVLS equipment.
PRC-011-0	R1.5.	Schedule for system maintenance.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for no more than 25% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 25% but less than or equal to 50% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 50% but less than or equal to 75% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 75% of the UVLS equipment.
PRC-011-0	R1.6.	Date last tested/maintained.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that the date last tested/maintained was missing for no more than 25% of	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 25% but	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 50% but	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 75% of

Complete Violation Severity Level Matrix (PRC) Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the UVLS equipment.	less than or equal to 50% of the UVLS equipment.	less than or equal to 75% of the UVLS equipment.	the UVLS equipment.
PRC-011-0	R2.	The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its UVLS equipment maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-015-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall maintain a list of and provide data for existing and proposed SPSs as specified in Reliability Standard PRC-013-0_R 1.	N/A	The responsible entity's list of existing or proposed SPSs did not address one of the elements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0 R1.	The responsible entity's list of existing or proposed SPSs did not address two of the elements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0 R1.	The responsible entity's list of existing or proposed SPSs did not address any of the elements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0 R1.
PRC-015-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have evidence it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures as defined in Reliability Standard PRC-012-0 R1 prior to being	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		placed in service.	procedures did not address one of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	procedures did not address two to four of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	procedures did not address five to seven of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	procedures did not address eight or more of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.
PRC-015-0	R3.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS data and the results of the studies that show compliance of new or functionally modified SPSs for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-016-0.1	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall analyze its SPS operations and maintain a record of all misoperations in accordance with the Regional SPS review procedure specified in Reliability Standard PRC-012-0_R 1.	The responsible entity was not compliant in that evidence that it analyzed its SPS operations and maintained a record of all misoperations in accordance with the Regional SPS	The responsible entity was not compliant in that evidence that it analyzed its SPS operations and maintained a record of all misoperations in accordance with the Regional SPS	The responsible entity was not compliant in that evidence that it analyzed its SPS operations and maintained a record of all misoperations in accordance with the Regional SPS	The responsible entity was not compliant in that evidence that it analyzed its SPS operations and maintained a record of all misoperations in accordance with the Regional SPS

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			review procedure did not address one of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1.	review procedure did not address two to four of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1.	review procedure did not address five to seven of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1.	review procedure did not address eight or more of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1.
PRC-016-0.1	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall take corrective actions to avoid future misoperations.	The responsible entity did not take corrective actions to avoid future SPS misoperations for no more than 25% of the events.	The responsible entity did not take corrective actions to avoid future SPS misoperations for more than 25% but less than or equal to 50% of the events.	The responsible entity did not take corrective actions to avoid future SPS misoperations for more than 50% but less than or equal to 75% of the events.	The responsible entity did not take corrective actions to avoid future SPS misoperations for more than 75% of the events.
PRC-016-0.1	R3.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days).	The responsible entity provided documentation of its SPS misoperation analyses and the corrective action plans more than 90 but less than or equal to 120 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS misoperation analyses and the corrective action plans more than 120 but less than or equal to 150 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS misoperation analyses and the corrective action plans more than 150 but less than or equal to 180 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS misoperation analyses and the corrective action plans more than 180 days following a request from its Regional Reliability Organization and/or NERC.
PRC-017-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have a system maintenance and testing program(s) in place. The	The responsible entity's SPS system maintenance and testing program did not address one of the elements in R1.1	The responsible entity's SPS system maintenance and testing program did not address two or three of the	The responsible entity's SPS system maintenance and testing program did not address four or five of the elements	The responsible entity's SPS system maintenance and testing program did not address any of the elements in R1.1

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		program(s) shall include:	through R1.6.	elements in R1.1 through R1.6.	in R1.1 through R1.6.	through R1.6.
PRC-017-0	R1.1.	SPS identification shall include but is not limited to:	The responsible entity's SPS program identification did not address one of the elements in R1.1.1 through R1.1.4.	The responsible entity's SPS program identification did not address two of the elements in R1.1.1 through R1.1.4.	The responsible entity's SPS program identification did not address three of the elements in R1.1.1 through R1.1.4.	The responsible entity's SPS program identification did not address any of the elements in R1.1.1 through R1.1.4.
PRC-017-0	R1.1.1.	Relays.	The responsible entity's SPS program identification was missing no more than 25% of the applicable relays.	The responsible entity's SPS program identification was missing more than 25% but less than or equal to 50% of the applicable relays.	The responsible entity's SPS program identification was missing more than 50% but less than or equal to 75% of the applicable relays.	The responsible entity's SPS program identification was missing more than 75% of the applicable relays.
PRC-017-0	R1.1.2.	Instrument transformers.	The responsible entity's SPS program identification was missing no more than 25% of the applicable instrument transformers.	The responsible entity's SPS program identification was missing more than 25% but less than or equal to 50% of the applicable instrument transformers.	The responsible entity's SPS program identification was missing more than 50% but less than or equal to 75% of the applicable instrument transformers.	The responsible entity's SPS program identification was missing more than 75% of the applicable instrument transformers.
PRC-017-0	R1.1.3.	Communications systems, where appropriate.	The responsible entity's SPS program identification was missing no more than 25% of the appropriate communication	The responsible entity's SPS program identification was missing more than 25% but less than or equal to 50% of the appropriate	The responsible entity's SPS program identification was missing more than 50% but less than or equal to 75% of the appropriate	The responsible entity's SPS program identification was missing more than 75% of the appropriate communication

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			systems.	communication systems.	communication systems.	systems.
PRC-017-0	R1.1.4.	Batteries.	The responsible entity's SPS program identification was missing no more than 25% of the applicable batteries.	The responsible entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the applicable batteries.	The responsible entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the applicable batteries.	The responsible entity's UVLS program system identification was missing more than 75% of the applicable batteries.
PRC-017-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	The responsible entity's SPS maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 75% of the SPS equipment.
PRC-017-0	R1.3.	Summary of testing procedure.	The responsible entity's SPS maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 25% but less than or equal to 50% of the SPS	The responsible entity's SPS maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 50% but less than or equal to 75% of the SPS	The responsible entity's SPS maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 75% of the SPS equipment.

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				equipment.	equipment.	
PRC-017-0	R1.4.	Schedule for system testing.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system testing was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 25% but less than or equal to 50% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 50% but less than or equal to 75% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 75% of the SPS equipment.
PRC-017-0	R1.5.	Schedule for system maintenance.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 25% but less than or equal to 50% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 50% but less than or equal to 75% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 75% of the SPS equipment.
PRC-017-0	R1.6.	Date last tested/maintained.	The responsible entity's SPS maintenance and testing program was non-compliant in that the date last tested/maintained was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 25% but less than or equal to	The responsible entity's SPS maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 50% but less than or equal to	The responsible entity's SPS maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 75% of the SPS equipment.

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				50% of the SPS equipment.	75% of the SPS equipment.	
PRC-017-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its SPS maintenance and testing program more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS maintenance and testing program more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS maintenance and testing program more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its SPS maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-018-1	R1.	Each Transmission Owner and Generator Owner required to install DMEs by its Regional Reliability Organization (reliability standard PRC-002 Requirements 1-3) shall have DMEs installed that meet the following requirements:	N/A	N/A	The responsible entity is not compliant in that the installation of DMEs does not include one of the elements in R1.1 and R1.2.	The responsible entity is not compliant in that the installation of DMEs does not include any of the elements in R1.1 and R1.2.
PRC-018-1	R1.1.	Internal Clocks in DME devices shall be synchronized to within 2 milliseconds or less of Universal Coordinated Time scale (UTC)	Less than or equal to 25% of DME devices did not comply with R1.1	Less than or equal to 37.5% but greater than 25% of DME devices did not comply with R1.1	Less than or equal to 50% but greater than 37.5% of DME devices did not comply with R1.1	Greater than 50% of DME devices did not comply with R1.1
PRC-018-1	R1.2.	Recorded data from each Disturbance shall be retrievable for ten calendar days.	Less than or equal to 12% of installed DME devices did not comply with R1.2	Less than or equal to 18% but greater than 12% of installed DME devices did not comply with R1.2	Less than or equal to 24% but greater than 18% of installed DME devices did not comply with R1.2	Greater than 24% of installed DME devices did not comply with R1.2
PRC-018-1	R2.	The Transmission Owner and Generator Owner shall each	The responsible entity is non-	The responsible entity is non-	The responsible entity is non-	The responsible entity is non-

Complete Violation Severity Level Matrix (PRC) Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		install DMEs in accordance with its Regional Reliability Organization's installation requirements (reliability standard PRC-002 Requirements 1 through 3).	compliant in that no more than 10% of the DME devices were not installed in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 Requirements 1 through 3.	compliant in that more than 10% but less than or equal to 20% of the DME devices were not installed in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 Requirements 1 through 3.	compliant in that more than 20% but less than or equal to 30% of the DME devices were not installed in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 Requirements 1 through 3.	compliant in that more than 30% of the DME devices were not installed in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 Requirements 1 through 3.
PRC-018-1	R3.	The Transmission Owner and Generator Owner shall each maintain, and report to its Regional Reliability Organization on request, the following data on the DMEs installed to meet that region's installation requirements (reliability standard PRC-002 Requirements 1.1, 2.1 and 3.1):	The responsible entity was not compliant in that evidence that it maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for one of the elements in Requirements 3.1 through 3.8.	The responsible entity was not compliant in that evidence that it maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for two or three of the elements in Requirements 3.1 through 3.8.	The responsible entity was not compliant in that evidence that it maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for four or five of the elements in Requirements 3.1 through 3.8.	The responsible entity was not compliant in that evidence that it maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for more than five of the elements in Requirements 3.1 through 3.8.
PRC-018-1	R3.1.	Type of DME (sequence of event recorder, fault recorder, or dynamic disturbance recorder).	Less than or equal to 25% of the required data per R3.1 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.1 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.1 was not maintained or reported.	Greater than 50% of the required data per R3.1 was not maintained or reported.

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-018-1	R3.2.	Make and model of equipment.	Less than or equal to 25% of the required data per R3.2 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.2 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.2 was not maintained or reported.	Greater than 50% of the required data per R3.2 was not maintained or reported.
PRC-018-1	R3.3.	Installation location.	Less than or equal to 25% of the required data per R3.3 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.3 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.3 was not maintained or reported.	Greater than 50% of the required data per R3.3 was not maintained or reported.
PRC-018-1	R3.4.	Operational status.	Less than or equal to 25% of the required data per R3.4 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.4 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.4 was not maintained or reported.	Greater than 50% of the required data per R3.4 was not maintained or reported.
PRC-018-1	R3.5.	Date last tested.	Less than or equal to 25% of the required data per R3.5 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.5 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.5 was not maintained or reported.	Greater than 50% of the required data per R3.5 was not maintained or reported.
PRC-018-1	R3.6.	Monitored elements, such as transmission circuit, bus section, etc.	Less than or equal to 25% of the required data per R3.6 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.6 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.6 was not maintained or reported.	Greater than 50% of the required data per R3.6 was not maintained or reported.
PRC-018-1	R3.7.	Monitored devices, such as circuit	Less than or equal	Less than or equal	Less than or equal	Greater than 50% of

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		breaker, disconnect status, alarms, etc.	to 25% of the required data per R3.7 was not maintained or reported.	to 37.5% but greater than 25% of the required data per R3.7 was not maintained or reported.	to 50% but greater than 37.5% of the required data per R3.7 was not maintained or reported.	the required data per R3.7 was not maintained or reported.
PRC-018-1	R3.8.	Monitored electrical quantities, such as voltage, current, etc.	Less than or equal to 25% of the required data per R3.8 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.8 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.8 was not maintained or reported.	Greater than 50% of the required data per R3.8 was not maintained or reported.
PRC-018-1	R4.	The Transmission Owner and Generator Owner shall each provide Disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements (reliability standard PRC-002 Requirement 4).	The responsible entity is not compliant in that it did not provide less than or equal to 10% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity is not compliant in that it did not provide less than or equal to 20% but greater than 10% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity is not compliant in that it did not provide less than or equal to 30% but greater than 20% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity is not compliant in that it did not provide greater than 30% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.
PRC-018-1	R5.	The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years.	The responsible entity is not compliant in that no more than 25% of the data recorded by DMEs for Regional Reliability Organization-identified events	The responsible entity is not compliant in that more than 25% but less than or equal to 50% of the data recorded by DMEs for Regional Reliability	The responsible entity is not compliant in that more than 50% but less than or equal to 75% of the data recorded by DMEs for Regional Reliability	The responsible entity is not compliant in that more than 75% of the data recorded by DMEs for Regional Reliability Organization-identified events

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			was not archived for at least three years.	Organization-identified events was not archived for at least three years.	Organization-identified events was not archived for at least three years.	was not archived for at least three years.
PRC-018-1	R6.	Each Transmission Owner and Generator Owner that is required by its Regional Reliability Organization to have DMEs shall have a maintenance and testing program for those DMEs that includes:	N/A	N/A	The responsible entity is not compliant in that the maintenance and testing program for DMEs does not include one of the elements in R6.1 and 6.2.	The responsible entity is not compliant in that the maintenance and testing program for DMEs does not include any of the elements in R6.1 and 6.2.
PRC-018-1	R6.1.	Maintenance and testing intervals and their basis.	The responsible entity's DME maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for no more than 25% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 75% of the DME equipment.
PRC-018-1	R6.2.	Summary of maintenance and testing procedures.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			missing for no more than 25% of the DME equipment.	missing for more than 25% but less than or equal to 50% of the DME equipment.	missing for more than 50% but less than or equal to 75% of the DME equipment.	missing for more than 75% of the DME equipment.
PRC-021-1	R1.	Each Transmission Owner and Distribution Provider that owns a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall annually update its UVLS data to support the Regional UVLS program database. The following data shall be provided to the Regional Reliability Organization for each installed UVLS system:	UVLS data was provided but did not address one of the elements in R1.1 through R1.5.	UVLS data was provided but did not address two of the elements in R1.1 through R1.5.	UVLS data was provided but did not address three of the elements in R1.1 through R1.5.	No annual UVLS data was provided OR UVLS data was provided but did not address four or more of the elements in R1.1 through R1.5.
PRC-021-1	R1.1.	Size and location of customer load, or percent of connected load, to be interrupted.	The responsible entity is non-compliant in the reporting of no more than 25% of the size or location of customer load, or percent of customer load to be interrupted.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of the size or location of customer load, or percent of customer load to be interrupted.	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of the size or location of customer load, or percent of customer load to be interrupted.	The responsible entity is non-compliant in the reporting of more than 75% of the size or location of customer load, or percent of customer load to be interrupted.
PRC-021-1	R1.2.	Corresponding voltage set points and overall scheme clearing times.	The responsible entity is non-compliant in the reporting of no more than 25% of the corresponding voltage set points and overall scheme clearing times.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of the corresponding voltage set points	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of the corresponding voltage set points	The responsible entity is non-compliant in the reporting of more than 75% of the corresponding voltage set points and overall scheme clearing times.

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				and overall scheme clearing times.	and overall scheme clearing times.	
PRC-021-1	R1.3.	Time delay from initiation to trip signal.	The responsible entity is non-compliant in the reporting of no more than 25% of the time delay from initiation to trip signal data.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of the time delay from initiation to trip signal data.	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of the time delay from initiation to trip signal data.	The responsible entity is non-compliant in the reporting of more than 75% of the time delay from initiation to trip signal data.
PRC-021-1	R1.4.	Breaker operating times.	The responsible entity is non-compliant in the reporting of no more than 25% of the breaker operating times.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of the breaker operating times.	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of the breaker operating times.	The responsible entity is non-compliant in the reporting of more than 75% of the breaker operating times.
PRC-021-1	R1.5.	Any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	The responsible entity is non-compliant in the reporting of no more than 25% of any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	The responsible entity is non-compliant in the reporting of more than 75% of any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.

Complete Violation Severity Level Matrix (PRC) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Systems.	Systems.	
PRC-021-1	R2.	Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request.	The responsible entity updated its UVLS data more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization.	The responsible entity updated its UVLS data more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization.	The responsible entity updated its UVLS data more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization.	The responsible entity did not update its UVLS data for more than 60 days following a request from its Regional Reliability Organization.
PRC-022-1	R1.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:	The responsible entity failed to analyze and document no more than 25% of all UVLS operations and misoperations.	The responsible entity failed to analyze and document more than 25% but less than or equal to 50% of all UVLS operations and misoperations or the overall analysis program did not address one of the elements in R1.1 through R1.5.	The responsible entity failed to analyze and document more than 50% but less than or equal to 75% of all UVLS operations and misoperations or the overall analysis program did not address two or three of the elements in R1.1 through R1.5.	The responsible entity failed to analyze and document more than 75% of all UVLS operations and misoperations or the overall analysis program did not address four or more of the elements in R1.1 through R1.5.
PRC-022-1	R1.1.	A description of the event including initiating conditions.	The responsible entity's analysis is missing a description of the event including initiating conditions for no more than 25% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a description of the event including initiating conditions for more than 25% but less than or equal to 50% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a description of the event including initiating conditions for more than 50% but less than or equal to 75% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a description of the event including initiating conditions for more than 75% of all UVLS operations and misoperations.
PRC-022-1	R1.2.	A review of the UVLS set points	The responsible	The responsible	The responsible	The responsible

Complete Violation Severity Level Matrix (PRC) Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and tripping times.	entity's analysis is missing a review of the UVLS set points and tripping times for no more than 25% of all UVLS operations and misoperations.	entity's analysis is missing a review of the UVLS set points and tripping times for more than 25% but less than 50% of all UVLS operations and misoperations.	entity's analysis is missing a review of the UVLS set points and tripping times for more than 50% but less than 75% of all UVLS operations and misoperations.	entity's analysis is missing a review of the UVLS set points and tripping times for more than 75% of all UVLS operations and misoperations.
PRC-022-1	R1.3.	A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.	The responsible entity's analysis is missing a simulation of the event, if deemed appropriate by the Regional Reliability Organization for no more than 25% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a simulation of the event, if deemed appropriate by the Regional Reliability Organization for more than 25% but less than or equal to 50% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a simulation of the event, if deemed appropriate by the Regional Reliability Organization for more than 50% but less than or equal to 75% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a simulation of the event, if deemed appropriate by the Regional Reliability Organization for more than 75% of all UVLS operations and misoperations.
PRC-022-1	R1.4.	A summary of the findings.	The responsible entity's analysis is missing a summary of the findings for no more than 25% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a summary of the findings for more than 25% but less than or equal to 50% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a summary of the findings for more than 50% but less than or equal to 75% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a summary of the findings for more than 75% of all UVLS operations and misoperations.
PRC-022-1	R1.5.	For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.	The responsible entity's analysis is missing a Corrective Action Plan to avoid future Misoperations of a	The responsible entity's analysis is missing a Corrective Action Plan to avoid future Misoperations of a	The responsible entity's analysis is missing a Corrective Action Plan to avoid future Misoperations of a	The responsible entity's analysis is missing a Corrective Action Plan to avoid future Misoperations of a

**Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			similar nature for no more than 25% of all UVLS operations and misoperations.	similar nature for more than 25% but less than or equal to 50% of all UVLS operations and misoperations.	similar nature for more than 50% but less than or equal to 75% of all UVLS operations and misoperations.	similar nature for more than 75% of all UVLS operations and misoperations.
PRC-022-1	R2.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.	The responsible entity provided documentation of the analysis of UVLS program performance more than 90 but less than or equal to 120 days following a request from its Regional Reliability Organization.	The responsible entity provided documentation of the analysis of UVLS program performance more than 120 but less than or equal to 150 days following a request from its Regional Reliability Organization.	The responsible entity provided documentation of the analysis of UVLS program performance more than 150 but less than or equal to 180 days following a request from its Regional Reliability Organization.	The responsible entity did not provide documentation of the analysis of UVLS program performance for more than 180 days following a request from its Regional Reliability Organization.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-001-1	R1.	Each Transmission Operator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its area and shall exercise specific authority to alleviate operating emergencies.	N/A	N/A	N/A	The Transmission Operator has no evidence that clear decision-making authority exists to assure reliability in its area or has failed to exercise this authority to alleviate operating emergencies.
TOP-001-1	R2.	Each Transmission Operator shall take immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.	N/A	N/A	N/A	The Transmission Operator failed to have evidence that it took immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.
TOP-001-1	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives	N/A	N/A	N/A	The responsible entity failed to comply with reliability directives issued by the Reliability Coordinator or the Transmission

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.				Operator (when applicable), when said directives would not have resulted in actions that would violate safety, equipment, regulatory or statutory requirements, or under circumstances that said directives would have resulted in actions that would violate safety, equipment, regulatory or statutory requirements the responsible entity failed to inform the Reliability Coordinator or Transmission Operator (when applicable) of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator could implement alternate remedial actions.
TOP-001-1	R4.	Each Distribution Provider and Load-Serving Entity shall	N/A	N/A	N/A	The responsible entity failed to

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions.</p>				<p>comply with all reliability directives issued by the Transmission Operator, including shedding firm load, when said directives would not have resulted in actions that would violate safety, equipment, regulatory or statutory requirements, or under circumstances when said directives would have violated safety, equipment, regulatory or statutory requirements, the responsible entity failed to immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator could implement alternate remedial actions.</p>
TOP-001-1	R5.	Each Transmission Operator shall inform its Reliability Coordinator and any other potentially affected Transmission	N/A	N/A	N/A	The Transmission Operator failed to inform its Reliability

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators of real-time or anticipated emergency conditions, and take actions to avoid, when possible, or mitigate the emergency.				Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, or failed to take actions to avoid, when possible, or mitigate the emergency.
TOP-001-1	R6.	Each Transmission Operator, Balancing Authority, and Generator Operator shall render all available emergency assistance to others as requested, provided that the requesting entity has implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements.	N/A	N/A	N/A	The responsible entity failed to render all available emergency assistance to others as requested, after the requesting entity had implemented its comparable emergency procedures, when said assistance would not have resulted in actions that would violate safety, equipment, or regulatory or statutory requirements.
TOP-001-1	R7.	Each Transmission Operator and Generator Operator shall not remove Bulk Electric System facilities from service if removing those facilities would	N/A	N/A	N/A	The responsible entity removed Bulk Electric System facilities from service under

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		burden neighboring systems unless:				conditions other than those listed in TOP-001-1 R7.1 through R7.3 and removal of said facilities burdened a neighboring system.
TOP-001-1	R7.1.	For a generator outage, the Generator Operator shall notify and coordinate with the Transmission Operator. The Transmission Operator shall notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	N/A	N/A	N/A	The Generator Operator failed to notify and coordinate with the Transmission Operator, or the Transmission Operator failed to notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.
TOP-001-1	R7.2.	For a transmission facility, the Transmission Operator shall notify and coordinate with its Reliability Coordinator. The Transmission Operator shall notify other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	N/A	N/A	N/A	The Transmission Operator failed to notify and coordinate with its Reliability Coordinator, or failed to notify other affected Transmission Operators, and coordinate the impact of removing

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the Bulk Electric System facility.
TOP-001-1	R7.3.	When time does not permit such notifications and coordination, or when immediate action is required to prevent a hazard to the public, lengthy customer service interruption, or damage to facilities, the Generator Operator shall notify the Transmission Operator, and the Transmission Operator shall notify its Reliability Coordinator and adjacent Transmission Operators, at the earliest possible time.	N/A	N/A	N/A	The Generator Operator failed to notify the Transmission Operator, or the Transmission Operator failed to notify its Reliability Coordinator and adjacent Transmission Operators during periods when time did not permit such notifications and coordination, or when immediate action was required to prevent a hazard to the public, lengthy customer service interruption, or damage to facilities.
TOP-001-1	R8.	During a system emergency, the Balancing Authority and Transmission Operator shall immediately take action to restore the Real and Reactive Power Balance. If the Balancing Authority or Transmission Operator is unable to restore Real and Reactive Power Balance it shall request emergency	N/A	N/A	N/A	The responsible entity failed to take immediate actions to restore the Real and Reactive Power Balance during a system emergency, or the responsible entity failed to request emergency

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		assistance from the Reliability Coordinator. If corrective action or emergency assistance is not adequate to mitigate the Real and Reactive Power Balance, then the Reliability Coordinator, Balancing Authority, and Transmission Operator shall implement firm load shedding.				assistance from the Reliability Coordinator during periods when it was unable to restore the Real and Reactive Power Balance, or during periods when corrective actions or emergency assistance was not adequate to mitigate the Real and Reactive Power Balance, the responsible entity failed to implement firm load shedding.
TOP-002-2	R1.	Each Balancing Authority and Transmission Operator shall maintain a set of current plans that are designed to evaluate options and set procedures for reliable operation through a reasonable future time period. In addition, each Balancing Authority and Transmission Operator shall be responsible for using available personnel and system equipment to implement these plans to ensure that interconnected system reliability will be maintained.	N/A	N/A	The responsible entity maintained a set of current plans that were designed to evaluate options and set procedures for reliable operation through a reasonable future time period, but failed utilize all available personnel and system equipment to implement these plans to ensure that interconnected system reliability	The responsible entity failed to maintain a set of current plans that were designed to evaluate options and set procedures for reliable operation through a reasonable future time period.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					will be maintained.	
TOP-002-2	R2.	Each Balancing Authority and Transmission Operator shall ensure its operating personnel participate in the system planning and design study processes, so that these studies contain the operating personnel perspective and system operating personnel are aware of the planning purpose.	N/A	N/A	N/A	The responsible entity failed to ensure its operating personnel participated in the system planning and design study processes.
TOP-002-2	R3.	Each Load-Serving Entity and Generator Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider. Each Balancing Authority and Transmission Service Provider shall coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.	N/A	The Load-Serving Entity or Generator Operator failed to coordinate (where confidentiality agreements allow) its seasonal operations with its Host Balancing Authority and Transmission Service Provider, or the Balancing Authority or Transmission Service Provider failed to coordinate its seasonal operations with its Transmission Operator.	N/A	The Load-Serving Entity or Generator Operator failed to coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider, or the Balancing Authority or Transmission Service Provider failed to coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.
TOP-002-2	R4.	Each Balancing Authority and Transmission Operator shall	N/A	The responsible entity failed to	N/A	The responsible entity failed to

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator, so that normal Interconnection operation will proceed in an orderly and consistent manner.		coordinate (where confidentiality agreements allow) its seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator.		coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator.
TOP-002-2	R5.	Each Balancing Authority and Transmission Operator shall plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.	N/A	N/A	N/A	The responsible entity failed to plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.
TOP-002-2	R6.	Each Balancing Authority and Transmission Operator shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional, and local reliability requirements.	N/A	N/A	N/A	The responsible entity failed to plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization,

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						subregional, and local reliability requirements.
TOP-002-2	R7.	Each Balancing Authority shall plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.
TOP-002-2	R8.	Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.
TOP-002-2	R9.	Each Balancing Authority shall plan to meet Interchange Schedules and Ramps.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet Interchange Schedules and Ramps.
TOP-002-2	R10.	Each Balancing Authority and Transmission Operator shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).	N/A	N/A	N/A	The responsible entity failed to plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-002-2	R11.	The Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs. Neighboring Transmission Operators shall utilize identical SOLs for common facilities. The Transmission Operator shall update these Bulk Electric System studies as necessary to reflect current system conditions; and shall make the results of Bulk Electric System studies available to the Transmission Operators, Balancing Authorities (subject confidentiality requirements), and to its Reliability Coordinator.	N/A	N/A	The Transmission Operator performed seasonal, next-day, and current-day Bulk Electric System studies, reflecting current system conditions, to determine SOLs, but failed to make the results of Bulk Electric System studies available to all of the Transmission Operators, Balancing Authorities (subject confidentiality requirements), or to its Reliability Coordinator.	The Transmission Operator failed to perform seasonal, next-day, or current-day Bulk Electric System studies, reflecting current system conditions, to determine SOLs.
TOP-002-2	R12.	The Transmission Service Provider shall include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available Transfer Capability calculation processes.	N/A	N/A	N/A	The Transmission Service Provider failed to include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Transfer Capability calculation processes.
TOP-002-2	R13.	At the request of the Balancing Authority or Transmission Operator, a Generator Operator shall perform generating real and reactive capability verification that shall include, among other variables, weather, ambient air and water conditions, and fuel quality and quantity, and provide the results to the Balancing Authority or Transmission Operator operating personnel as requested.	N/A	N/A	N/A	The Generator Operator failed to perform generating real and reactive capability verification that included, among other variables, weather, ambient air and water conditions, and fuel quality and quantity, or failed to provide the results of generating real and reactive verifications Balancing Authority or Transmission Operator operating personnel, when requested.
TOP-002-2	R14.	Generator Operators shall, without any intentional time delay, notify their Balancing Authority and Transmission Operator of changes in capabilities and characteristics including but not limited to:	N/A	N/A	N/A	The Generator Operator failed to notify their Balancing Authority and Transmission Operator of changes in capabilities and characteristics.
TOP-002-2	R14.1.	Changes in real output capabilities.	N/A	N/A	N/A	The Generator Operator failed to notify its Balancing

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Authority or Transmission Operator of changes in real output capabilities.
TOP-002-2	R14.2.	Automatic Voltage Regulator status and mode setting. (Retired August 1, 2007)				
TOP-002-2	R15.	Generation Operators shall, at the request of the Balancing Authority or Transmission Operator, provide a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).	N/A	N/A	N/A	The Generation Operator failed to provide, at the request of the Balancing Authority or Transmission Operator, a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).
TOP-002-2	R16.	Subject to standards of conduct and confidentiality agreements, Transmission Operators shall, without any intentional time delay, notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics including but not limited to:	N/A	N/A	N/A	The Transmission Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2	R16.1.	Changes in transmission facility	N/A	N/A	N/A	The Transmission

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		status.				Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in transmission facility status, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2	R16.2.	Changes in transmission facility rating.	N/A	N/A	N/A	The Transmission Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in transmission facility rating, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2	R17.	Balancing Authorities and Transmission Operators shall, without any intentional time delay, communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.	N/A	N/A	N/A	The responsible entity failed to communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-002-2	R18.	Neighboring Balancing Authorities, Transmission Operators, Generator Operators, Transmission Service Providers, and Load-Serving Entities shall use uniform line identifiers when referring to transmission facilities of an interconnected network.	N/A	N/A	N/A	The responsible entity failed to use uniform line identifiers when referring to transmission facilities of an interconnected network.
TOP-002-2	R19.	Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations.	N/A	N/A	N/A	The responsible entity failed to maintain accurate computer models utilized for analyzing and planning system operations.
TOP-003-0	R1.	Generator Operators and Transmission Operators shall provide planned outage information.				
TOP-003-0	R1.1.	Each Generator Operator shall provide outage information daily to its Transmission Operator for scheduled generator outages planned for the next day (any foreseen outage of a generator greater than 50 MW). The Transmission Operator shall establish the outage reporting requirements.	N/A	N/A	N/A	The Generator Operator failed to provide outage information, in accordance with its Transmission Operators established outage reporting requirements, to its Transmission Operator for scheduled generator outages planned for the next day (any

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						foreseen outage of a generator greater than 50 MW).
TOP-003-0	R1.2.	Each Transmission Operator shall provide outage information daily to its Reliability Coordinator, and to affected Balancing Authorities and Transmission Operators for scheduled generator and bulk transmission outages planned for the next day (any foreseen outage of a transmission line or transformer greater than 100 kV or generator greater than 50 MW) that may collectively cause or contribute to an SOL or IROL violation or a regional operating area limitation. The Reliability Coordinator shall establish the outage reporting requirements.	N/A	N/A	N/A	The Transmission Operator failed to provide outage information, in accordance with its Reliability Coordinators established outage reporting requirement, to its Reliability Coordinator, and to affected Balancing Authorities and Transmission Operators for scheduled generator and bulk transmission outages planned for the next day (any foreseen outage of a transmission line or transformer greater than 100 kV or generator greater than 50 MW) that may collectively cause or contribute to an SOL or IROL violation or a regional operating area limitation.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-003-0	R1.3.	Such information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.	N/A	N/A	N/A	The responsible entity failed to provide the information by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.
TOP-003-0	R2.	Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of system voltage regulating equipment, such as automatic voltage regulators on generators, supplementary excitation control, synchronous condensers, shunt and series capacitors, reactors, etc., among affected Balancing Authorities and Transmission Operators as required.	N/A	N/A	N/A	The responsible entity failed to plan or coordinate scheduled outages of system voltage regulating equipment, such as automatic voltage regulators on generators, supplementary excitation control, synchronous condensers, shunt and series capacitors, reactors, etc., among affected Balancing Authorities and Transmission Operators when required.
TOP-003-0	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall plan	The responsible entity planned and coordinated	N/A	N/A	The responsible entity failed to plan and coordinate

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and coordinate scheduled outages of telemetering and control equipment and associated communication channels between the affected areas.	scheduled outages of telemetering and control equipment and associated communication channels with its Reliability Coordinator, but failed to coordinate with affected neighboring Transmission Operators, Balancing Authorities, and Generator Operators.			scheduled outages of telemetering and control equipment and associated communication channels between the affected areas.
TOP-003-0	R4.	Each Reliability Coordinator shall resolve any scheduling of potential reliability conflicts.	N/A	N/A	N/A	The Reliability Coordinator failed to resolve any scheduling of potential reliability conflicts.
TOP-004-1	R1.	Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).	N/A	N/A	The Transmission Operator operated within the Interconnection Reliability Operating Limits (IROLs), but failed to operate within the System Operating Limits (SOLs).	The Transmission Operator failed to operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).
TOP-004-1	R2.	Each Transmission Operator shall operate so that instability, uncontrolled separation, or	N/A	N/A	N/A	The Transmission Operator failed to operate so that

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cascading outages will not occur as a result of the most severe single contingency.				instability, uncontrolled separation, or cascading outages would not occur as a result of the most severe single contingency.
TOP-004-1	R3.	Each Transmission Operator shall, when practical, operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by Regional Reliability Organization policy.	N/A	N/A	N/A	The Transmission Operator failed to operate (when practical) to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by Regional Reliability Organization policy.
TOP-004-1	R4.	If a Transmission Operator enters an unknown operating state (i.e., any state for which valid operating limits have not been determined), it will be considered to be in an emergency and shall restore operations to respect proven reliable power system limits within 30 minutes.	The Transmission Operator entering an unknown operating state (i.e., any state for which valid operating limits have not been determined), failed to restore operations to respect proven reliable power system limits for more than 30 minutes but less than or equal to 35	The Transmission Operator entering an unknown operating state (i.e., any state for which valid operating limits have not been determined), failed to restore operations to respect proven reliable power system limits for more than 35 minutes but less than or equal to 40	The Transmission Operator entering an unknown operating state (i.e., any state for which valid operating limits have not been determined), failed to restore operations to respect proven reliable power system limits for more than 40 minutes but less than or equal to 45	The Transmission Operator entering an unknown operating state (i.e., any state for which valid operating limits have not been determined), failed to restore operations to respect proven reliable power system limits for more than 45 minutes.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			minutes.	minutes.	minutes.	
TOP-004-1	R5.	Each Transmission Operator shall make every effort to remain connected to the Interconnection. If the Transmission Operator determines that by remaining interconnected, it is in imminent danger of violating an IROL or SOL, the Transmission Operator may take such actions, as it deems necessary, to protect its area.	N/A	N/A	N/A	The Transmission Operator does not have evidence that the actions taken to protect its area, resulting in its disconnection from the Interconnection, were necessary to prevent the danger of violating an IROL or SOL.
TOP-004-1	R6.	Transmission Operators, individually and jointly with other Transmission Operators, shall develop, maintain, and implement formal policies and procedures to provide for transmission reliability. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including:	The Transmission Operator developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, including the elements listed in TOP-004-1 R6.1 through R6.6, but failed to include other Transmission Operators in the development of said	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include one of the elements listed in TOP-004-1	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include two of the elements listed in TOP-004-1	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include three or more of the elements listed in

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			policies and procedures.	R6.1 through R6.6.	R6.1 through R6.6.	TOP-004-1 R6.1 through R6.6.
TOP-004-1	R6.1.	Equipment ratings.	The Transmission Operator failed to include equipment ratings in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.	N/A	N/A	N/A
TOP-004-1	R6.2.	Monitoring and controlling voltage levels and real and reactive power flows.	The Transmission Operator failed to include monitoring and controlling voltage levels and real and reactive power flows in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.	N/A	N/A	N/A
TOP-004-1	R6.3.	Switching transmission elements.	The Transmission Operator failed to include switching	N/A	N/A	N/A

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			transmission elements in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.			
TOP-004-1	R6.4.	Planned outages of transmission elements.	The Transmission Operator failed to include planned outages of transmission elements in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.	N/A	N/A	N/A
TOP-004-1	R6.5.	Development of IROLs and SOLs.	The Transmission Operator failed to include development of IROLs and SOLs in the development, maintenance, and implementation of formal policies and	N/A	N/A	N/A

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			procedures to provide for transmission reliability as described in TOP-004-1 R6.			
TOP-004-1	R6.6.	Responding to IROL and SOL violations.	The Transmission Operator failed to include responding to IROL and SOL violations in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.	N/A	N/A	N/A
TOP-005-1.1	R1.	Each Transmission Operator and Balancing Authority shall provide its Reliability Coordinator with the operating data that the Reliability Coordinator requires to perform operational reliability assessments and to coordinate reliable operations within the Reliability Coordinator Area.	The responsible entity failed to provide all of the data requested by its Reliability Coordinator.	N/A	N/A	The responsible entity failed to provide all of the data requested by its Reliability Coordinator.
TOP-005-1.1	R1.1.	Each Reliability Coordinator shall identify the data requirements from the list in Attachment 1-TOP-005-0 "Electric System Reliability	N/A	N/A	N/A	The Reliability Coordinator failed to identify the data necessary to perform operational

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Data” and any additional operating information requirements relating to operation of the bulk power system within the Reliability Coordinator Area.				reliability assessments and to coordinate reliable operations within the Reliability Coordinator Area.
TOP-005-1.1	R2.	As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for “Electric System Reliability Data.”	N/A	N/A	N/A	The ISN data recipient failed to sign the NERC Confidentiality Agreement for “Electric System Reliability Data”.
TOP-005-1.1	R3.	Upon request, each Balancing Authority and Transmission Operator shall provide to other Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability, the operating data that are necessary to allow these Balancing Authorities and Transmission Operators to perform operational reliability assessments and to coordinate reliable operations. Balancing Authorities and Transmission Operators shall provide the types of data as listed in Attachment 1-TOP-005-0 “Electric System Reliability Data,” unless otherwise agreed to by the Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability.	The responsible entity failed to provide any of the data requested by other Balancing Authorities or Transmission Operators.	N/A	N/A	The responsible entity failed to provide all of the data requested by its host Balancing Authority or Transmission Operator.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-005-1.1	R4.	Each Purchasing-Selling Entity shall provide information as requested by its Host Balancing Authorities and Transmission Operators to enable them to conduct operational reliability assessments and coordinate reliable operations.	The responsible entity failed to provide any of the data requested by other Balancing Authorities or Transmission Operators.	N/A	N/A	The responsible entity failed to provide all of the data requested by its host Balancing Authority or Transmission Operator.
TOP-006-1	R1.	Each Transmission Operator and Balancing Authority shall know the status of all generation and transmission resources available for use.	N/A	N/A	N/A	The responsible entity failed to know the status of all generation and transmission resources available for use, even though said information was reported by the Generator Operator, Transmission Operator, or Balancing Authority.
TOP-006-1	R1.1.	Each Generator Operator shall inform its Host Balancing Authority and the Transmission Operator of all generation resources available for use.	N/A	N/A	N/A	The Generator Operator failed to inform its Host Balancing Authority and the Transmission Operator of all generation resources available for use.
TOP-006-1	R1.2.	Each Transmission Operator and Balancing Authority shall inform the Reliability Coordinator and other affected Balancing Authorities and Transmission	N/A	N/A	N/A	The responsible entity failed to inform the Reliability Coordinator and

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators of all generation and transmission resources available for use.				other affected Balancing Authorities and Transmission Operators of all generation and transmission resources available for use.
TOP-006-1	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources.	N/A	The responsible entity monitors the applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, but is not aware of the status of rotating and static reactive resources.	The responsible entity fails to monitor all of the applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of all rotating and static reactive resources.	The responsible entity fails to monitor any of the applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources.
TOP-006-1	R3.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide appropriate technical information concerning protective relays to their operating personnel.	The responsible entity failed to provide any of the appropriate technical information concerning protective relays to their operating personnel.	N/A	N/A	The responsible entity failed to provide all of the appropriate technical information concerning protective relays to their operating personnel.
TOP-006-1	R4.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have information, including weather forecasts and past load patterns,	N/A	N/A	The responsible entity has either weather forecasts or past load patterns, available to predict	The responsible entity failed to have both weather forecasts and past load patterns,

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		available to predict the system's near-term load pattern.			the system's near-term load pattern, but not both.	available to predict the system's near-term load pattern.
TOP-006-1	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions and to indicate, if appropriate, the need for corrective action.	N/A	N/A	The responsible entity used monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions, but does not have indication of the need for corrective action.	The responsible entity failed to use monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions.
TOP-006-1	R6.	Each Balancing Authority and Transmission Operator shall use sufficient metering of suitable range, accuracy and sampling rate (if applicable) to ensure accurate and timely monitoring of operating conditions under both normal and emergency situations.	N/A	N/A	N/A	The responsible entity failed to use sufficient metering of suitable range, accuracy and sampling rate (if applicable) to ensure accurate and timely monitoring of operating conditions under both normal and emergency situations.
TOP-006-1	R7.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor system frequency.	N/A	N/A	N/A	The responsible entity failed to monitor system frequency.
TOP-007-0	R1.	A Transmission Operator shall inform its Reliability Coordinator when an IROL or SOL has been exceeded and the actions being	N/A	N/A	The Transmission Operator informed its Reliability Coordinator when	The Transmission Operator failed to inform its Reliability

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		taken to return the system to within limits.			an IROL or SOL had been exceeded but failed to provide the actions being taken to return the system to within limits.	Coordinator when an IROL or SOL had been exceeded.
TOP-007-0	R2.	Following a Contingency or other event that results in an IROL violation, the Transmission Operator shall return its transmission system to within IROL as soon as possible, but not longer than 30 minutes.	Following a Contingency or other event that resulted in an IROL violation of a magnitude up to and including 5%, the Transmission Operator failed to return its transmission system to within IROL in less than or equal to 35 minutes.	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within IROL in accordance with the following: (a) an IROL with a magnitude up to and including 5% for a period of time greater than 35 minutes but less than or equal to 45 minutes, or (b) an IROL with a magnitude greater than 5% but less than or equal to 10% for a period of time less than or equal to 40 minutes, or (c) an IROL with a magnitude greater	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within IROL in accordance with the following: (a) an IROL with a magnitude up to and including 5% for a period of time greater than 45 minutes, or (b) an IROL with a magnitude greater than 5% but less than or equal to 10% for a period of time greater than 40 minutes, or (c) an IROL with a magnitude greater than 10% but less than or equal to 15%	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within IROL in accordance with the following: (a) an IROL with a magnitude greater than 10% but less than or equal to 15% for a period of time greater than 45 minutes, or (b) an IROL with a magnitude greater than 15% but less than or equal to 20% for a period of time greater than 40 minutes, or (c) an IROL with a magnitude greater than 20% but less

**Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				than 10% but less than or equal to 15% for a period of time less than or equal to 35 minutes.	for a period of time greater than 35 minutes but less than or equal to 45 minutes, or (d) an IROL with a magnitude greater than 15% but less than or equal to 20% for a period of time less than or equal to 40 minutes, or (e) an IROL with a magnitude greater than 20% but less than or equal to 25% for a period of time less than or equal to 35 minutes.	than or equal to 25% for a period of time greater than 35 minutes, or (d) an IROL with a magnitude greater than 25% for a period of greater than 30 minutes.
TOP-007-0	R3.	A Transmission Operator shall take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to comply with Requirement R 2.	N/A	N/A	N/A	The Transmission Operator failed to take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to return the transmission system to IROL within 30 minutes.
TOP-007-0	R4.	The Reliability Coordinator shall evaluate actions taken to address an IROL or SOL violation and, if the actions taken are not	N/A	N/A	N/A	The Reliability Coordinator failed to evaluate actions taken to address an

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		appropriate or sufficient, direct actions required to return the system to within limits.				IROL or SOL violation and, if the actions taken were not appropriate or sufficient, direct actions required to return the system to within limits.
TOP-008-1	R1.	The Transmission Operator experiencing or contributing to an IROL or SOL violation shall take immediate steps to relieve the condition, which may include shedding firm load.	N/A	N/A	N/A	The Transmission Operator experiencing or contributing to an IROL or SOL violation failed to take immediate steps to relieve the condition, which may have included shedding firm load.
TOP-008-1	R2.	Each Transmission Operator shall operate to prevent the likelihood that a disturbance, action, or inaction will result in an IROL or SOL violation in its area or another area of the Interconnection. In instances where there is a difference in derived operating limits, the Transmission Operator shall always operate the Bulk Electric System to the most limiting parameter.	N/A	The Transmission Operator operated to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area or another area of the Interconnection but failed to operate the Bulk Electric System to the most limiting parameter in instances where there was a	The Transmission Operator operated to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area but failed to operate to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in another area of the Interconnection.	The Transmission Operator failed to operate to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area or another area of the Interconnection.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				difference in derived operating limits.		
TOP-008-1	R3.	The Transmission Operator shall disconnect the affected facility if the overload on a transmission facility or abnormal voltage or reactive condition persists and equipment is endangered. In doing so, the Transmission Operator shall notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection prior to switching, if time permits, otherwise, immediately thereafter.	N/A	The Transmission Operator disconnected the affected facility when the overload on a transmission facility or abnormal voltage or reactive condition persisted and equipment was endangered but failed to notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection either prior to switching, if time permitted, otherwise, immediately thereafter.	N/A	The Transmission Operator failed to disconnect the affected facility when the overload on a transmission facility or abnormal voltage or reactive condition persisted and equipment was endangered.
TOP-008-1	R4.	The Transmission Operator shall have sufficient information and analysis tools to determine the cause(s) of SOL violations. This analysis shall be conducted in all operating timeframes. The Transmission Operator shall use the results of these analyses to immediately mitigate the SOL violation.	N/A	N/A	The Transmission Operator had sufficient information and analysis tools to determine the cause(s) of SOL violations and used the results of these analyses to	The Transmission Operator failed to have sufficient information and analysis tools to determine the cause(s) of SOL violations or failed to use the results of analyses to

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					immediately mitigate the SOL violation(s), but failed to conduct these analyses in all operating timeframes.	immediately mitigate the SOL violation.

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-001-0.1	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that, with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services at all Demand levels over the range of forecast system demands, under the conditions defined in Category A of Table I. To be considered valid, the Planning Authority and Transmission Planner assessments shall:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-001-0.1	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-001-0.1	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-001-	R1.3.	Be supported by a current or	The responsible	The responsible entity	The responsible	The responsible entity

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
0.1		past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category A of Table 1 (no contingencies). The specific elements selected (from each of the following categories) shall be acceptable to the associated Regional Reliability Organization(s).	entity is non-compliant with 25% or less of the sub-components.	is non-compliant with more than 25% but less than 50% of the sub-components.	entity is non-compliant with 50% or more but less than 75% of the sub-components.	is non-compliant with 75% or more of the sub-components.
TPL-001-0.1	R1.3.1.	Cover critical system conditions and study years as deemed appropriate by the entity performing the study.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-001-0.1	R1.3.2.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system testing) AND most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-001-0.1	R1.3.3.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system simulation testing show marginal conditions that may require longer lead-time solutions.
TPL-001-0.1	R1.3.4.	Have established normal (pre-contingency) operating procedures in place.	N/A	N/A	N/A	No precontingency operating procedures are in place for existing facilities.
TPL-001-0.1	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-001-0.1	R1.3.6.	Be performed for selected demand levels over the range of forecast system demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						over a range of forecast system demands.
TPL-001-0.1	R1.3.7.	Demonstrate that system performance meets Table 1 for Category A (no contingencies).	N/A	N/A	N/A	No past or current study results exist showing pre-contingency system analysis.
TPL-001-0.1	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-001-0.1	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-001-0.1	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category A.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category A planning

Complete Violation Severity Level Matrix (TPL) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						requirements.
TPL-001-0.1	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-001-0_R1, the Planning Authority and Transmission Planner shall each:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-001-0.1	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon.	N/A	N/A	N/A	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category A planning requirements.
TPL-001-0.1	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	A schedule for the responsible entity's corrective action plan does not exist.
TPL-001-0.1	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	Anticipated in-service dates, for the responsible entity's corrective action plan do not exist.
TPL-001-0.1	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	The responsible entity failed to consider necessary lead times to implement its corrective action plan.
TPL-001-0.1	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed	N/A	N/A	N/A	The responsible entity has failed to demonstrate the continuing need for previously identified

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implementation plans are not needed.				facility additions through subsequent annual assessments.
TPL-001-0.1	R3.	The Planning Authority and Transmission Planner shall each document the results of these reliability assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization
TPL-002-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I. To be valid, the Planning Authority and Transmission Planner assessments shall:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Complete Violation Severity Level Matrix (TPL) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-002-0	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-002-0	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-002-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category B of Table 1 (single contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-002-0	R1.3.1.	Be performed and evaluated only for those Category B contingencies that would produce the more severe System results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce	N/A	The responsible entity provided evidence through current or past studies and/or system simulation testing that selected NERC Category B contingencies were evaluated, however, no rationale was provided to indicate	N/A	The responsible entity did not provide evidence through current or past studies and/or system simulation testing to indicate that any NERC Category B contingencies were evaluated.

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		less severe system results shall be available as supporting information.		why the remaining Category B contingencies for their system were not evaluated.		
TPL-002-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-002-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system simulation testing) AND most recent long-term studies (and/or system testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system simulation testing) are no longer valid.
TPL-002-0	R1.3.4.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						planning horizon) when past or current year near-term studies and/or system simulation testing show marginal conditions that may require longer lead-time solutions.
TPL-002-0	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-002-0	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast system Demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-002-0	R1.3.7.	Demonstrate that system performance meets Category B contingencies.	N/A	N/A	N/A	No past or current study results exist showing Category B contingency system analysis.
TPL-002-0	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past	The responsible entity's transmission model used for past or	N/A	The responsible entity's transmission model used for past or

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.		current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-002-0	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-002-0	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-002-0	R1.3.11.	Include the effects of existing and planned control devices.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned control devices.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing control devices.

Complete Violation Severity Level Matrix (TPL) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-002-0	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-002-0	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category B of Table I.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category B planning requirements.
TPL-002-0	R1.5.	Consider all contingencies applicable to Category B.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to 25% or less of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient 75% or more of all applicable contingencies.
TPL-002-0	R2.	When System simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-002-0_R1, the Planning Authority and Transmission Planner shall	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		each:				
TPL-002-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	N/A	N/A	N/A	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category B planning requirements.
TPL-002-0	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	A schedule for the responsible entity's corrective action plan does not exist.
TPL-002-0	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	Anticipated in-service dates, for the responsible entity's corrective action plan does not exist. This would reflect effective dates for pre-contingency operating procedures or in-service dates for proposed system changes.
TPL-002-0	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	The responsible entity failed to consider necessary lead times to implement its corrective action plan.
TPL-002-0	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not	N/A	N/A	N/A	The responsible entity has failed to demonstrate the continuing need for previously identified facility additions

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		needed.				through sub-sequent annual assessments.
TPL-002-0	R3.	The Planning Authority and Transmission Planner shall each document the results of its Reliability Assessments and corrective plans and shall annually provide the results to its respective Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization
TPL-003-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Complete Violation Severity Level Matrix (TPL) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard. To be valid, the Planning Authority and Transmission Planner assessments shall:				
TPL-003-0	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-003-0	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-003-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category C of Table 1 (multiple contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-003-0	R1.3.1.	Be performed and evaluated only for those Category C	N/A	The responsible entity provided evidence	N/A	The responsible entity did not provided

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.		through current or past studies that selected NERC Category C contingencies were evaluated, however, no rational was provided to indicate why the remaining Category C contingencies for their system were not evaluated.		evidence through current or past studies to indicate that any NERC Category C contingencies were evaluated.
TPL-003-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-003-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system simulation testing) AND most recent long-term studies (and/or system testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system simulation testing) are

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						no longer valid.
TPL-003-0	R1.3.4.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system testing show marginal conditions that may require longer lead-time solutions.
TPL-003-0	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-003-0	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast system demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-003-0	R1.3.7.	Demonstrate that System	N/A	N/A	N/A	No past or current

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		performance meets Table 1 for Category C contingencies.				study results exists showing Category C contingency system analysis.
TPL-003-0	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-003-0	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet System performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-003-0	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-003-0	R1.3.11.	Include the effects of existing	N/A	N/A	The responsible	The responsible

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and planned control devices.			entity's transmission model used for past or current studies is deficient with respect to the effects of planned control devices.	entity's transmission model used for past or current studies is deficient with respect to the effects of existing control devices.
TPL-003-0	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those Demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-003-0	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category C.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category C planning requirements.
TPL-003-0	R1.5.	Consider all contingencies applicable to Category C.	The responsible entity has considered the NERC Category C contingencies applicable to their system, but was deficient with respect to 25% or less of all applicable contingencies.	The responsible entity has considered the NERC Category C contingencies applicable to their system, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	The responsible entity has considered the NERC Category C contingencies applicable to their system, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	The responsible entity has considered the NERC Category C contingencies applicable to their system, but was deficient 75% or more of all applicable contingencies.

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-003-0	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-003-0_R1, the Planning Authority and Transmission Planner shall each:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-003-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	N/A	N/A	N/A	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category C planning requirements.
TPL-003-0	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	A schedule for the responsible entity's corrective action plan does not exist.
TPL-003-0	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	Anticipated in-service dates, for the responsible entity's corrective action plan does not exist. This would reflect effective dates for pre-contingency operating procedures or in-service dates for proposed system changes.
TPL-003-0	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	The responsible entity failed to consider necessary lead times to implement its

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						corrective action plan.
TPL-003-0	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	N/A	N/A	N/A	The responsible entity has failed to demonstrate the continuing need for previously identified facility additions through sub-sequent annual assessments.
TPL-003-0	R3.	The Planning Authority and Transmission Planner shall each document the results of these Reliability Assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization
TPL-004-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is evaluated for the risks and consequences of a number of each of the extreme contingencies that are listed under Category D of Table I. To be valid, the Planning Authority's and Transmission	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Planner's assessment shall:				
TPL-004-0	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-004-0	R1.2.	Be conducted for near-term (years one through five).	N/A	N/A	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period.
TPL-004-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category D contingencies of Table I. The specific elements selected (from within each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-004-0	R1.3.1.	Be performed and evaluated only for those Category D contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting	N/A	The responsible entity provided evidence through current or past studies that selected NERC Category D contingencies were evaluated, however, no rationale was provided to indicate why the remaining Category D contingencies for their	N/A	The responsible entity did not provide evidence through current or past studies to indicate that any NERC Category D contingencies were evaluated.

Complete Violation Severity Level Matrix (TPL) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		information.		system were not evaluated.		
TPL-004-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-004-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	N/A	N/A	N/A	The responsible entity did not perform a near-term Category D study and/or system simulation test in the most recent annual period AND system changes (actual or proposed) indicate that past studies and/or system simulation testing are no longer valid
TPL-004-0	R1.3.4.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-004-0	R1.3.5.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			properly reflects existing facilities, but is deficient in reflecting planned facilities.	reflects planned facilities, but is deficient in reflecting existing facilities.		reflecting existing AND planned facilities.
TPL-004-0	R1.3.6.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-004-0	R1.3.7.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-004-0	R1.3.8.	Include the effects of existing and planned control devices.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned control devices.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing control devices.
TPL-004-0	R1.3.9.	Include the planned (including maintenance) outage of any bulk electric equipment	N/A	N/A	N/A	The responsible entity's transmission model used for past or

**Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.				current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-004-0	R1.4.	Consider all contingencies applicable to Category D.	The responsible entity has considered the NERC Category D contingencies, but was deficient with respect to 25% or less of all applicable contingencies	The responsible entity has considered the NERC Category D contingencies, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	The responsible entity has considered the NERC Category D contingencies, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	The responsible entity has considered the NERC Category D contingencies, but was deficient 75% or more of all applicable contingencies.
TPL-004-0	R2.	The Planning Authority and Transmission Planner shall each document the results of its reliability assessments and shall annually provide the results to its entities' respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments but did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments AND did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization

**Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-001-1	R1.	Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting 5% or less of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting between 5-10% of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting 10-15%, inclusive, of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting greater than 15% of their individual and neighboring areas voltage levels and Mvar flows.
VAR-001-1	R2.	Each Transmission Operator shall acquire sufficient reactive resources within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 95% but less than 100% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 90% but less than 95% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 85% but less than 90% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired less than 85% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.
VAR-001-1	R3.	The Transmission Operator	N/A	N/A	N/A	The Transmission

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.				Operator did not specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1. to all of the parties involved.
VAR-001-1	R3.1.	Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing one or more entities. The missing entities shall represent less than 25% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing two or more entities. The missing entities shall represent less than 50% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing three or more entities. The missing entities shall represent less than 75% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing four or more entities. The missing entities shall represent 75% or more of those eligible for the list.
VAR-001-1	R3.2.	For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.	The Transmission Operator failed to notify up to 25% of the associated Generator Owner of each generator that are on this exemption list.	The Transmission Operator failed to notify 25% up to 50% of the associated Generator Owners of each generator that are on this exemption list.	The Transmission Operator failed to notify 50% up to 75% of the associated Generator Owner of each generator that are on this exemption list.	The Transmission Operator failed to notify 75% up to 100% of the associated Generator Owner of each generator that are on this exemption list.
VAR-001-1	R4.	Each Transmission Operator shall specify a voltage or Reactive Power schedule at	N/A	N/A	The Transmission Operator provide Voltage or Reactive Power schedules	The Transmission Operator provide No evidence that voltage or Reactive Power

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).			were for some but not all generating units as required in R4.	schedules were provided to Generator Operators as required in R4.
VAR-001-1	R5.	Each Purchasing-Selling Entity shall arrange for (self-provide or purchase) reactive resources to satisfy its reactive requirements identified by its Transmission Service Provider.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting 5% or less of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting between 5-10% of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting 10-15%, inclusive, of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting greater than 15% of its reactive requirements.
VAR-001-1	R6.	The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting

**Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			requirement, affecting 5% or less of the required resources.	directed by the requirement, affecting between 5-10% of the required resources.	requirement, affecting 10-15%, inclusive, of the required resources.	15% or greater of required resources.
VAR-001-1	R6.1.	When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.	N/A	N/A	N/A	The Transmission Operator has not provided evidence to show that directives were issued to the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule in accordance with R6.1.
VAR-001-1	R7.	The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting 5% or less of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting between 5-10% of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting 10-15%, inclusive, of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting greater than 15% of the required devices.
VAR-001-1	R8.	Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources	The applicable entity did operate or direct the operation of capacitive and	The applicable entity did operate or direct the operation of	The applicable entity did operate or direct the operation of capacitive and	The applicable entity did operate or direct the operation of capacitive and

**Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		within its area – including reactive generation scheduling; transmission line and reactive resource switching; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.	inductive reactive resources or load shedding within its area, as directed by the requirement, affecting 5% or less of the required resources.	capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting between 5-10% of the required resources.	inductive reactive resources or load shedding within its area, as directed by the requirement, affecting 10-15%, inclusive, of the required resources.	inductive reactive resources or load shedding within its area, as directed by the requirement, affecting greater than 15% of the required resources.
VAR-001-1	R9.	Each Transmission Operator shall maintain reactive resources to support its voltage under first Contingency conditions.	The Transmission Operator maintains 95% or more of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains 85% or more but less than 95% of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains 75% or more but less than 85% of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains less than 75% of the reactive resources needed to support its voltage under first Contingency conditions.
VAR-001-1	R9.1.	Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.	The applicable entity did not disperse and/or locate the reactive resources, as directed in the requirement, affecting 5% or less of the resources.	The applicable entity did not disperse and/or locate the reactive resources, as directed in the requirement, affecting between 5-10% of the resources.	The applicable entity did not disperse and/or locate the reactive resources, as directed in the requirement, affecting 10-15%, inclusive, of the resources.	The applicable entity did not disperse and/or locate the reactive resources, as directed in the requirement, affecting greater than 15% of the resources.
VAR-001-1	R10.	Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies	The applicable entity did not correct the IROL or SOL violations and/or	The applicable entity did not correct the IROL or SOL violations	The applicable entity did not correct the IROL or SOL violations and/or	The applicable entity did not correct the IROL or SOL violations and/or

**Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.	complete the required IROL or SOL violation reporting, as directed by the requirement, affecting 5% or less of the violations.	and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting between 5-10% of the violations.	complete the required IROL or SOL violation reporting, as directed by the requirement, affecting 10-15%, inclusive, of the violations.	complete the required IROL or SOL violation reporting, as directed by the requirement, affecting greater than 15% of the violations.
VAR-001-1	R11.	After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.	The Transmission Operator provided documentation to the Generator Owner specifying required step-up transformer tap changes and a timeframe for making these changes, but failed to provide technical justification for these changes.	The Transmission Operator provided documentation to the Generator Owner specifying required step-up transformer tap changes, but failed to provide a timeframe for making these changes and technical justification for these changes.	The Transmission Operator failed to provide documentation to the Generator Owner specifying required step-up transformer tap changes, a timeframe for making these changes, and technical justification for these changes.	N/A
VAR-001-1	R12.	The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.	N/A	N/A	N/A	The Transmission Operator has failed to direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.
VAR-002-	R1.	The Generator Operator	The Generator	The Generator	The Generator	The Generator

Complete Violation Severity Level Matrix (VAR) **Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
1.1a		shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator.	Operator failed to notify the Transmission Operator as identified in R1 for less than 25% of its generators.	Operator failed to notify the Transmission Operator as identified in R1 for 25% or more but less than 50% of its generators.	Operator failed to notify the Transmission Operator as identified in R1 for 50% or more but less than 75% of its generators.	Operator failed to notify the Transmission Operator as identified in R1 for 75% or more of its generators.
VAR-002-1.1a	R2.	Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings. [1] as directed by the Transmission Operator	The Generator Operator failed to maintain a voltage or reactive power schedule for less than 25% of its generators.	The Generator Operator failed to maintain a voltage or reactive power schedule for 25% or more but less than 50% of its generators.	The Generator Operator failed to maintain a voltage or reactive power schedule for 50% or more but less than 75% of its generators.	The Generator Operator failed to maintain a voltage or reactive power schedule for 75% or more of its generators.
VAR-002-1.1a	R2.1.	When a generator's automatic voltage regulator is out of service, the Generator Operator shall use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.	The Generator Operator failed to use an alternate method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule for less than 25% of its generators.	The Generator Operator failed to use an alternate method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule for 25% or more but less than 50% of its generators.	The Generator Operator failed to use an alternate method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule for 50% or more but less than 75% of its generators.	The Generator Operator failed to use an alternate method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule for 75% or more of its generators.
VAR-002-1.1a	R2.2.	When directed to modify voltage, the Generator	The Generator Operator failed to	The Generator Operator failed to	The Generator Operator failed to	The Generator Operator failed to

**Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operator shall comply or provide an explanation of why the schedule cannot be met.	comply with required voltage modifications or provide an explanation of why the modifications could not be met less the 25% of the time.	comply with required voltage modifications or provide an explanation of why the modifications could not be met less than 50% of the time but more than or equal to 25% of the time.	comply with required voltage modifications or provide an explanation of why the modifications could not be met less than 75% of the time but more than or equal to 50% of the time.	comply with required voltage modifications or provide an explanation of why the modifications could not be met more than 75% of the time.
VAR-002-1.1a	R3.	Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:	The Generator Operator had one incident of failing to notify the Transmission Operator as identified in R3.	The Generator Operator had more than one but less than five incidents of failing to notify the Transmission as identified in R3.1 R3.2.	The Generator Operator had more than five but less than ten incidents of failing to notify the Transmission Operator as identified in R3.1 R3.2	The Generator Operator had ten or more incidents of failing to notify the Transmission Operator as identified in R3.1 R3.2.
VAR-002-1.1a	R3.1.	A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.	N/A	N/A	N/A	The Generator Operator failed to notify the Transmission Operator of a status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.

**Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1a	R3.2.	A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.	N/A	N/A	N/A	The Generator Operator failed to notify the Transmission Operator of a status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.
VAR-002-1.1a	R4.	The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.	The Generator Owner had one (1) incident of failing to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.	The Generator Owner had more than one (1) incident but less than five (5) incidents of failing to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.	The Generator Owner had more than five (5) incidents but less than ten (10) incidents of failing to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.	The Generator Owner had more than ten (10) incidents of failing to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.

**Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				than the generator terminal voltage.		
VAR-002-1.1a	R4.1.	For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.
VAR-002-1.1a	R4.1.1.	Tap settings.	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for tap settings on generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.

**Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1a	R4.1.2.	Available fixed tap ranges.	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for available fixed tap ranges on generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.
VAR-002-1.1a	R4.1.3.	Impedance data.	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for impedance data on generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.
VAR-002-1.1a	R4.1.4.	The +/- voltage range with step-change in % for load-tap changing transformers.	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Planner within 30 calendar days of a request for the +/- voltage range with tap change in percent (%) for load-tap changing transformers on generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.
VAR-002-1.1a	R5.	After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.	The Generator Owner had one (1) incident of failing to change the step-up transformer tap settings in accordance with the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.	The Generator Owner had more than one (1) incident but less than or equal to five (5) incidents of failing to change the step-up transformer tap settings in accordance with the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.	The Generator Owner had more than five (5) incident but less than or equal to ten (10) incidents of failing to change the step-up transformer tap settings in accordance with the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.	The Generator Owner had more than ten (10) incidents of failing to change the step-up transformer tap settings in accordance with the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.
VAR-002-	R5.1.	If the Generator Operator	The Generator	The Generator	The Generator	The Generator

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
1.1a		can't comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.	Operator had one (1) incident of failing to notify and provide technical justification to the Transmission Operator concerning non-compliance with Transmission Operator's specifications.	Operator had more than one (1) incident but less than or equal to five (5) incidents of failing to notify and provide technical justification to the Transmission Operator concerning non-compliance with Transmission Operator's specifications.	Operator had more than five (5) incident but less than or equal to ten (10) incidents of failing to notify and provide technical justification to the Transmission Operator concerning non-compliance with Transmission Operator's specifications.	Operator had more than ten (10) incidents of failing to notify and provide technical justification to the Transmission Operator concerning non-compliance with Transmission Operator's specifications.

Exhibit E

Complete Matrix of Violation Risk Factors for Approved Reliability Standards

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-001-0.1a	R1.	Each Balancing Authority shall operate such that, on a rolling 12-month basis, the average of the clock-minute averages of the Balancing Authority's Area Control Error (ACE) divided by 10B (B is the clock-minute average of the Balancing Authority Area's Frequency Bias) times the corresponding clock-minute averages of the Interconnection's Frequency Error is less than a specific limit. This limit $\square_1 \square$ is a constant derived from a targeted frequency bound (separately calculated for each Interconnection) that is reviewed and set as necessary by the NERC Operating Committee. <i>See Standard for Formula.</i>	MEDIUM
BAL-001-0.1a	R2.	Each Balancing Authority shall operate such that its average ACE for at least 90% of clock-ten-minute periods (6 non-overlapping periods per hour) during a calendar month is within a specific limit, referred to as L_{10} . <i>See Standard for Formula.</i>	MEDIUM
BAL-001-0.1a	R3.	Each Balancing Authority providing Overlap Regulation Service shall evaluate Requirement R1 (i.e., Control Performance Standard 1 or CPS1) and Requirement R2 (i.e., Control Performance Standard 2 or CPS2) using the characteristics of the combined ACE and combined Frequency Bias Settings.	LOWER
BAL-001-0.1a	R4.	Any Balancing Authority receiving Overlap Regulation Service shall not have its control performance evaluated (i.e. from a control performance perspective, the Balancing Authority has shifted all control requirements to the Balancing Authority providing Overlap Regulation Service).	LOWER
BAL-002-0	R1.	Each Balancing Authority shall have access to and/or operate Contingency Reserve to respond to Disturbances. Contingency Reserve may be supplied from generation, controllable load resources, or coordinated adjustments to Interchange Schedules.	HIGH
BAL-002-0	R1.1.	A Balancing Authority may elect to fulfill its Contingency Reserve obligations by participating as a member of a Reserve Sharing Group. In such cases, the Reserve Sharing Group shall have the same responsibilities and obligations as each Balancing Authority with respect to monitoring and meeting the requirements of Standard BAL-002.	HIGH
BAL-002-0	R2.	Each Regional Reliability Organization, sub-Regional Reliability Organization or Reserve Sharing Group shall specify its Contingency Reserve policies, including:	MEDIUM
BAL-002-0	R2.1.	The minimum reserve requirement for the group.	HIGH
BAL-002-0	R2.2.	Its allocation among members.	LOWER
BAL-002-0	R2.3.	The permissible mix of Operating Reserve – Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.	LOWER
BAL-002-0	R2.4.	The procedure for applying Contingency Reserve in practice.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-002-0	R2.5.	The limitations, if any, upon the amount of interruptible load that may be included.	LOWER
BAL-002-0	R2.6.	The same portion of resource capacity (e.g., reserves from jointly owned generation) shall not be counted more than once as Contingency Reserve by multiple Balancing Authorities.	MEDIUM
BAL-002-0	R3.	Each Balancing Authority or Reserve Sharing Group shall activate sufficient Contingency Reserve to comply with the DCS.	HIGH
BAL-002-0	R3.1.	As a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency. All Balancing Authorities and Reserve Sharing Groups shall review, no less frequently than annually, their probable contingencies to determine their prospective most severe single contingencies.	HIGH
BAL-002-0	R4.	A Balancing Authority or Reserve Sharing Group shall meet the Disturbance Recovery Criterion within the Disturbance Recovery Period for 100% of Reportable Disturbances. The Disturbance Recovery Criterion is:	MEDIUM
BAL-002-0	R4.1.	A Balancing Authority shall return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to zero. For negative initial ACE values just prior to the Disturbance, the Balancing Authority shall return ACE to its pre-Disturbance value.	MEDIUM
BAL-002-0	R4.2.	The default Disturbance Recovery Period is 15 minutes after the start of a Reportable Disturbance. This period may be adjusted to better suit the needs of an Interconnection based on analysis approved by the NERC Operating Committee.	<blank>
BAL-002-0	R5.	Each Reserve Sharing Group shall comply with the DCS. A Reserve Sharing Group shall be considered in a Reportable Disturbance condition whenever a group member has experienced a Reportable Disturbance and calls for the activation of Contingency Reserves from one or more other group members. (If a group member has experienced a Reportable Disturbance but does not call for reserve activation from other members of the Reserve Sharing Group, then that member shall report as a single Balancing Authority.) Compliance may be demonstrated by either of the following two methods:	LOWER
BAL-002-0	R5.1.	The Reserve Sharing Group reviews group ACE (or equivalent) and demonstrates compliance to the DCS. To be in compliance, the group ACE (or its equivalent) must meet the Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.	<blank>
BAL-002-0	R5.2.	The Reserve Sharing Group reviews each member's ACE in response to the activation of reserves. To be in compliance, a member's ACE (or its equivalent) must meet the Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.	<blank>

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-002-0	R6.	A Balancing Authority or Reserve Sharing Group shall fully restore its Contingency Reserves within the Contingency Reserve Restoration Period for its Interconnection.	MEDIUM
BAL-002-0	R6.1.	The Contingency Reserve Restoration Period begins at the end of the Disturbance Recovery Period.	<blank>
BAL-002-0	R6.2.	The default Contingency Reserve Restoration Period is 90 minutes. This period may be adjusted to better suit the reliability targets of the Interconnection based on analysis approved by the NERC Operating Committee.	<blank>
BAL-003-0.1b	R1.	Each Balancing Authority shall review its Frequency Bias Settings by January 1 of each year and recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.	LOWER
BAL-003-0.1b	R1.1.	The Balancing Authority may change its Frequency Bias Setting, and the method used to determine the setting, whenever any of the factors used to determine the current bias value change.	LOWER
BAL-003-0.1b	R1.2.	Each Balancing Authority shall report its Frequency Bias Setting, and method for determining that setting, to the NERC Operating Committee.	LOWER
BAL-003-0.1b	R2.	Each Balancing Authority shall establish and maintain a Frequency Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response. Frequency Bias may be calculated several ways:	MEDIUM
BAL-003-0.1b	R2.1.	The Balancing Authority may use a fixed Frequency Bias value which is based on a fixed, straight-line function of Tie Line deviation versus Frequency Deviation. The Balancing Authority shall determine the fixed value by observing and averaging the Frequency Response for several Disturbances during on-peak hours.	LOWER
BAL-003-0.1b	R2.2.	The Balancing Authority may use a variable (linear or non-linear) bias value, which is based on a variable function of Tie Line deviation to Frequency Deviation. The Balancing Authority shall determine the variable frequency bias value by analyzing Frequency Response as it varies with factors such as load, generation, governor characteristics, and frequency.	LOWER
BAL-003-0.1b	R3.	Each Balancing Authority shall operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, unless such operation is adverse to system or Interconnection reliability.	MEDIUM
BAL-003-0.1b	R4.	Balancing Authorities that use Dynamic Scheduling or Pseudo-ties for jointly owned units shall reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-003-0.1b	R4.1.	Fixed schedules for Jointly Owned Units mandate that Balancing Authority (A) that contains the Jointly Owned Unit must incorporate the respective share of the unit governor droop response for any Balancing Authorities that have fixed schedules (B and C). See the diagram below. <i>See Standard for Graphic.</i>	LOWER
BAL-003-0	R4.2.	The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit shall not include their share of the governor droop response in their Frequency Bias Setting. <i>See Standard for Graphic.</i>	LOWER
BAL-003-0.1b	R5.	Balancing Authorities that serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change.	MEDIUM
BAL-003-0.1b	R5.1.	Balancing Authorities that do not serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.	MEDIUM
BAL-003-0.1b	R6.	A Balancing Authority that is performing Overlap Regulation Service shall increase its Frequency Bias Setting to match the frequency response of the entire area being controlled. A Balancing Authority shall not change its Frequency Bias Setting when performing Supplemental Regulation Service.	MEDIUM
BAL-004-WECC-01	R1.	Each BA that operates synchronously to the Western Interconnection shall continuously operate utilizing Automatic Time Error Correction (ATEC) in its Automatic Generation Control (AGC) system. <i>See Standard for Formula</i>	LOWER
BAL-004-WECC-01	R1.2.	Large accumulations of primary inadvertent point to an invalid implementation of ATEC, loose control, metering or accounting errors. A BA in such a situation should identify the source of the error(s) and make the corrections, recalculate the primary inadvertent from the time of the error, adjust the accumulated primary inadvertent caused by the error(s), validate the implementation of ATEC, set Lmax equal to L10 and continue to operate with ATEC reducing the accumulation as system parameters allow.	
BAL-004-WECC-01	R2.	Each BA that is synchronously connected to the Western Interconnection and operates in any AGC operating mode other than ATEC shall notify all other BAs of its operating mode through the designated Interconnection communication system. Each BA while synchronously connected to the Western Interconnection will be allowed to have ATEC out of service for a maximum of 24 hours per calendar quarter, for reasons including maintenance and testing.	LOWER
BAL-004-WECC-01	R3.	BAs in the Western Interconnection shall be able to change their AGC operating mode between Flat Frequency (for blackout restoration); Flat Tie Line (for loss of frequency telemetry); Tie Line Bias; Tie Line Bias plus Time Error control (used in ATEC mode). The ACE used for NERC reports shall be the same ACE as the AGC operating mode in use.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-004-WECC-01	R4.	Regardless of the AGC operating mode each BA in the Western Interconnection shall compute its hourly Primary Inadvertent Interchange when hourly checkout is complete. If hourly checkout is not complete by 50 minutes after the hour, compute Primary Inadvertent Interchange with best available data. This hourly value shall be added to the appropriate accumulated Primary Inadvertent Interchange balance for either On-Peak or Off-Peak periods.	LOWER
BAL-004-WECC-01	R4.1.	Each BA in the Western Interconnection shall use the change in Time Error distributed by the Interconnection Time Monitor.	
BAL-004-WECC-01	R4.2.	All corrections to any previous hour Primary Inadvertent Interchange shall be added to the appropriate On- or Off-Peak accumulated Primary Inadvertent Interchange.	
BAL-004-WECC-01	R4.3.	Month end Inadvertent Adjustments are 100% Primary Inadvertent Interchange and shall be added to the appropriate On- or Off-Peak accumulated Primary Inadvertent Interchange, unless such adjustments can be pinpointed to specific hours in which case R4.2 applies.	
BAL-004-WECC-01	R4.4.	Each BA in the Western Interconnection shall synchronize its Time Error to the nearest 0.001 seconds of the system Time Error by comparing its reading at the designated time each day to the reading broadcast by the Interconnection Time Monitor. Any difference shall be applied as an adjustment to its current Time Error.	
BAL-004-0	R1.	Only a Reliability Coordinator shall be eligible to act as Interconnection Time Monitor. A single Reliability Coordinator in each Interconnection shall be designated by the NERC Operating Committee to serve as Interconnection Time Monitor.	LOWER
BAL-004-0	R2.	The Interconnection Time Monitor shall monitor Time Error and shall initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.	LOWER
BAL-004-0	R3.	Each Balancing Authority, when requested, shall participate in a Time Error Correction by one of the following methods:	MEDIUM
BAL-004-0	R3.1.	The Balancing Authority shall offset its frequency schedule by 0.02 Hertz, leaving the Frequency Bias Setting normal; or	LOWER
BAL-004-0	R3.2.	The Balancing Authority shall offset its Net Interchange Schedule (MW) by an amount equal to the computed bias contribution during a 0.02 Hertz Frequency Deviation (i.e. 20% of the Frequency Bias Setting).	LOWER
BAL-004-0	R4.	Any Reliability Coordinator in an Interconnection shall have the authority to request the Interconnection Time Monitor to terminate a Time Error Correction in progress, or a scheduled Time Error Correction that has not begun, for reliability considerations.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-004-0	R4.1.	Balancing Authorities that have reliability concerns with the execution of a Time Error Correction shall notify their Reliability Coordinator and request the termination of a Time Error Correction in progress.	LOWER
BAL-005-0.1b	R1.	All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.	<blank>
BAL-005-0.1b	R1.1.	Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.	MEDIUM
BAL-005-0.1b	R1.2.	Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.	MEDIUM
BAL-005-0.1b	R1.3.	Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.	MEDIUM
BAL-005-0.1b	R2.	Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.	HIGH
BAL-005-0.1b	R3.	A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.	MEDIUM
BAL-005-0.1b	R4.	A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.	MEDIUM
BAL-005-0.1b	R5.	A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.	MEDIUM
BAL-005-0.1b	R6.	The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.	MEDIUM
BAL-005-0.1b	R7.	The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-005-0.1b	R8.	The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.	MEDIUM
BAL-005-0.1b	R8.1.	Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.	MEDIUM
BAL-005-0.1b	R9.	The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.	LOWER
BAL-005-0.1b	R9.1.	Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.	LOWER
BAL-005-0.1b	R10.	The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.	HIGH
BAL-005-0.1b	R11.	Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.	MEDIUM
BAL-005-0.1b	R12.	Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.	MEDIUM
BAL-005-0.1b	R12.1.	Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.	LOWER
BAL-005-0.1b	R12.2.	Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.	MEDIUM
BAL-005-0.1b	R12.3.	Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.	MEDIUM
BAL-005-0.1b	R13.	Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-005-0.1b	R14.	The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.	LOWER
BAL-005-0.1b	R15.	The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.	LOWER
BAL-005-0.1b	R16.	The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.	MEDIUM
BAL-005-0.1b	R17.	Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below: <i>See Standard for Values</i>	MEDIUM
BAL-006-1.1	R1.	Each Balancing Authority shall calculate and record hourly Inadvertent Interchange.	LOWER
BAL-006-1.1	R2.	Each Balancing Authority shall include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. The Balancing Authority shall take into account interchange served by jointly owned generators.	LOWER
BAL-006-1.1	R3.	Each Balancing Authority shall ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.	LOWER
BAL-006-1.1	R4.	Adjacent Balancing Authority Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign. Each Balancing Authority shall compute its Inadvertent Interchange based on the following:	LOWER
BAL-006-1.1	R4.1.	Each Balancing Authority, by the end of the next business day, shall agree with its Adjacent Balancing Authorities to:	LOWER
BAL-006-1.1	R4.1.1.	The hourly values of Net Interchange Schedule.	LOWER
BAL-006-1.1	R4.1.2.	The hourly integrated megawatt-hour values of Net Actual Interchange.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
BAL-006-1.1	R4.2.	Each Balancing Authority shall use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.	LOWER
BAL-006-1.1	R4.3.	A Balancing Authority shall make after-the-fact corrections to the agreed-to daily and monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). Changes or corrections based on non-reliability considerations shall not be reflected in the Balancing Authority's Inadvertent Interchange. After-the-fact corrections to scheduled or actual values will not be accepted without agreement of the Adjacent Balancing Authority(ies).	LOWER
BAL-006-1.1	R5.	Adjacent Balancing Authorities that cannot mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month shall, for the purposes of dispute resolution, submit a report to their respective Regional Reliability Organization Survey Contact. The report shall describe the nature and the cause of the dispute as well as a process for correcting the discrepancy.	LOWER
CIP-001-1	R1.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	MEDIUM
CIP-001-1	R2.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	MEDIUM
CIP-001-1	R3.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	MEDIUM
CIP-001-1	R4.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	MEDIUM
CIP-002-1	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	MEDIUM
CIP-002-1	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	LOWER
CIP-002-1	R1.2.	The risk-based assessment shall consider the following assets:	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-002-1	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	LOWER
CIP-002-1	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.4.	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	LOWER
CIP-002-1	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	LOWER
CIP-002-1	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.7.	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	LOWER
CIP-002-1	R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	HIGH
CIP-002-1	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	HIGH
CIP-002-1	R3.1.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	LOWER
CIP-002-1	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	LOWER
CIP-002-1	R3.3.	The Cyber Asset is dial-up accessible.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-002-1	R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	LOWER
CIP-003-1	R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	MEDIUM
CIP-003-1	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.	LOWER
CIP-003-1	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	LOWER
CIP-003-1	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-1	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009	MEDIUM
CIP-003-1	R2.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	LOWER
CIP-003-1	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-1	R2.3.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-1	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	LOWER
CIP-003-1	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	LOWER
CIP-003-1	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-003-1	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	LOWER
CIP-003-1	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-1	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	MEDIUM
CIP-003-1	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	LOWER
CIP-003-1	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	LOWER
CIP-003-1	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-1	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	LOWER
CIP-003-1	R5.1.1.	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	LOWER
CIP-003-1	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-1	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	LOWER
CIP-003-1	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-003-1	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	LOWER
CIP-004-1	R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: Direct communications (e.g., emails, memos, computer based training, etc.); Indirect communications (e.g., posters, intranet, brochures, etc.); Management support and reinforcement (e.g., presentations, meetings, etc.).	LOWER
CIP-004-1	R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	LOWER
CIP-004-1	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	MEDIUM
CIP-004-1	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-1	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-1	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-1	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-1	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	LOWER
CIP-004-1	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-004-1	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	MEDIUM
CIP-004-1	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and sevenyear criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	LOWER
CIP-004-1	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	LOWER
CIP-004-1	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.	LOWER
CIP-004-1	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	LOWER
CIP-004-1	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	LOWER
CIP-004-1	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	MEDIUM
CIP-005-1	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	MEDIUM
CIP-005-1	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-005-1	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	MEDIUM
CIP-005-1	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-1	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	MEDIUM
CIP-005-1	R1.5.	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	MEDIUM
CIP-005-1	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	LOWER
CIP-005-1	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-1	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	MEDIUM
CIP-005-1	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	MEDIUM
CIP-005-1	R2.3.	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-1	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	MEDIUM
CIP-005-1	R2.5.	The required documentation shall, at least, identify and describe:	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-005-1	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-1	R2.5.2.	The authentication methods.	LOWER
CIP-005-1	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.	LOWER
CIP-005-1	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-1	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	LOWER
CIP-005-1	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	MEDIUM
CIP-005-1	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	MEDIUM
CIP-005-1	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	MEDIUM
CIP-005-1	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	MEDIUM
CIP-005-1	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-1	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-1	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-1	R4.4.	A review of controls for default accounts, passwords, and network management community strings; and,	MEDIUM
CIP-005-1	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-005-1	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	LOWER
CIP-005-1	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.	LOWER
CIP-005-1	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	LOWER
CIP-005-1	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	LOWER
CIP-006-1	R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-1	R1.1.	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.	MEDIUM
CIP-006-1	R1.2.	Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-1	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-1	R1.4.	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-1	R1.5.	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	MEDIUM
CIP-006-1	R1.6.	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-1	R1.7.	Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-006-1	R1.8.	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	LOWER
CIP-006-1	R1.9.	Process for ensuring that the physical security plan is reviewed at least annually.	LOWER
CIP-006-1	R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	MEDIUM
CIP-006-1	R2.1.	Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.	MEDIUM
CIP-006-1	R2.2.	Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.	MEDIUM
CIP-006-1	R2.3.	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	MEDIUM
CIP-006-1	R2.4.	Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	MEDIUM
CIP-006-1	R3.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	MEDIUM
CIP-006-1	R3.1.	Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.	MEDIUM
CIP-006-1	R3.2.	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.	LOWER
CIP-006-1	R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-006-1	R4.1.	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	LOWER
CIP-006-1	R4.2.	Video Recording: Electronic capture of video images of sufficient quality to determine identity.	LOWER
CIP-006-1	R4.3.	Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.	LOWER
CIP-006-1	R5.	Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	LOWER
CIP-006-1	R6.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-1	R6.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-1	R6.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	LOWER
CIP-006-1	R6.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-1	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	MEDIUM
CIP-007-1	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	MEDIUM
CIP-007-1	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-1	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-1	R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-007-1	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MEDIUM
CIP-007-1	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	MEDIUM
CIP-007-1	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	MEDIUM
CIP-007-1	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	LOWER
CIP-007-1	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	LOWER
CIP-007-1	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER
CIP-007-1	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	MEDIUM
CIP-007-1	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	MEDIUM
CIP-007-1	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.	MEDIUM
CIP-007-1	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-007-1	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.	MEDIUM
CIP-007-1	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	LOWER
CIP-007-1	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	LOWER
CIP-007-1	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.	MEDIUM
CIP-007-1	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	LOWER
CIP-007-1	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	MEDIUM
CIP-007-1	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-1	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	MEDIUM
CIP-007-1	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-1	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-1	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-1	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-1	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-007-1	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	MEDIUM
CIP-007-1	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-1	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.	MEDIUM
CIP-007-1	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-1	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-1	R7.	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	LOWER
CIP-007-1	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-1	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-1	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-1	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	LOWER
CIP-007-1	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-1	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	MEDIUM
CIP-007-1	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-1	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-007-1	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	LOWER
CIP-008-1	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	LOWER
CIP-008-1	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER
CIP-008-1	R1.2.	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	LOWER
CIP-008-1	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.	LOWER
CIP-008-1	R1.4.	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	LOWER
CIP-008-1	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-1	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-1	R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	LOWER
CIP-009-1	R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	MEDIUM
CIP-009-1	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	MEDIUM
CIP-009-1	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-1	R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
CIP-009-1	R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	LOWER
CIP-009-1	R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	LOWER
CIP-009-1	R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	LOWER
COM-001-1	R1.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information:	HIGH
COM-001-1.1	R1.1.	Internally.	HIGH
COM-001-1.1	R1.2.	Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.	HIGH
COM-001-1.1	R1.3.	With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.	HIGH
COM-001-1.1	R1.4.	Where applicable, these facilities shall be redundant and diversely routed.	HIGH
COM-001-1.1	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.	MEDIUM
COM-001-1.1	R3.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate telecommunications among their respective areas. This coordination shall include the ability to investigate and recommend solutions to telecommunications problems within the area and with other areas.	LOWER
COM-001-1.1	R4.	Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing Authorities may use an alternate language for internal operations.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
COM-001-1.1	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.	LOWER
COM-001-1.1	R6.	Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."	LOWER
COM-002-2	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. Such communications shall be staffed and available for addressing a real-time emergency condition.	HIGH
COM-002-2	R1.1.	Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator, and all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.	HIGH
COM-002-2	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall issue directives in a clear, concise, and definitive manner; shall ensure the recipient of the directive repeats the information back correctly; and shall acknowledge the response as correct or repeat the original statement to resolve any misunderstandings.	MEDIUM
EOP-001-0	R1.	Balancing Authorities shall have operating agreements with adjacent Balancing Authorities that shall, at a minimum, contain provisions for emergency assistance, including provisions to obtain emergency assistance from remote Balancing Authorities.	HIGH
EOP-001-0	R2.	The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. The plan shall include the details on how the Transmission Operator will implement load reduction in sufficient amount and time to mitigate the IROL violation before system separation or collapse would occur. The load reduction plan must be capable of being implemented within 30 minutes.	MEDIUM
EOP-001-0	R3.	Each Transmission Operator and Balancing Authority shall:	MEDIUM
EOP-001-0	R3.1.	Develop, maintain, and implement a set of plans to mitigate operating emergencies for insufficient generating capacity.	MEDIUM
EOP-001-0	R3.2.	Develop, maintain, and implement a set of plans to mitigate operating emergencies on the transmission system.	MEDIUM
EOP-001-0	R3.3.	Develop, maintain, and implement a set of plans for load shedding.	MEDIUM
EOP-001-0	R3.4.	Develop, maintain, and implement a set of plans for system restoration.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
EOP-001-0	R4.	Each Transmission Operator and Balancing Authority shall have emergency plans that will enable it to mitigate operating emergencies. At a minimum, Transmission Operator and Balancing Authority emergency plans shall include:	MEDIUM
EOP-001-0	R4.1.	Communications protocols to be used during emergencies.	MEDIUM
EOP-001-0	R4.2.	A list of controlling actions to resolve the emergency. Load reduction, in sufficient quantity to resolve the emergency within NERC-established timelines, shall be one of the controlling actions.	MEDIUM
EOP-001-0	R4.3.	The tasks to be coordinated with and among adjacent Transmission Operators and Balancing Authorities.	MEDIUM
EOP-001-0	R4.4.	Staffing levels for the emergency.	MEDIUM
EOP-001-0	R5.	Each Transmission Operator and Balancing Authority shall include the applicable elements in Attachment 1-EOP-001-0 when developing an emergency plan.	MEDIUM
EOP-001-0	R6.	The Transmission Operator and Balancing Authority shall annually review and update each emergency plan. The Transmission Operator and Balancing Authority shall provide a copy of its updated emergency plans to its Reliability Coordinator and to neighboring Transmission Operators and Balancing Authorities.	MEDIUM
EOP-001-0	R7.	The Transmission Operator and Balancing Authority shall coordinate its emergency plans with other Transmission Operators and Balancing Authorities as appropriate. This coordination includes the following steps, as applicable:	MEDIUM
EOP-001-0	R7.1.	The Transmission Operator and Balancing Authority shall establish and maintain reliable communications between interconnected systems.	MEDIUM
EOP-001-0	R7.2.	The Transmission Operator and Balancing Authority shall arrange new interchange agreements to provide for emergency capacity or energy transfers if existing agreements cannot be used.	MEDIUM
EOP-001-0	R7.3.	The Transmission Operator and Balancing Authority shall coordinate transmission and generator maintenance schedules to maximize capacity or conserve the fuel in short supply. (This includes water for hydro generators.)	MEDIUM
EOP-001-0	R7.4.	The Transmission Operator and Balancing Authority shall arrange deliveries of electrical energy or fuel from remote systems through normal operating channels.	MEDIUM
EOP-002-2	R1.	Each Balancing Authority and Reliability Coordinator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its respective area and shall exercise specific authority to alleviate capacity and energy emergencies.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
EOP-002-2	R2.	Each Balancing Authority shall implement its capacity and energy emergency plan, when required and as appropriate, to reduce risks to the interconnected system.	HIGH
EOP-002-2	R3.	A Balancing Authority that is experiencing an operating capacity or energy emergency shall communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.	HIGH
EOP-002-2	R4.	A Balancing Authority anticipating an operating capacity or energy emergency shall perform all actions necessary including bringing on all available generation, postponing equipment maintenance, scheduling interchange purchases in advance, and being prepared to reduce firm load.	HIGH
EOP-002-2	R5.	A deficient Balancing Authority shall only use the assistance provided by the Interconnection's frequency bias for the time needed to implement corrective actions. The Balancing Authority shall not unilaterally adjust generation in an attempt to return Interconnection frequency to normal beyond that supplied through frequency bias action and Interchange Schedule changes. Such unilateral adjustment may overload transmission facilities.	HIGH
EOP-002-2	R6.	If the Balancing Authority cannot comply with the Control Performance and Disturbance Control Standards, then it shall immediately implement remedies to do so. These remedies include, but are not limited to:	HIGH
EOP-002-2	R6.1.	Loading all available generating capacity.	HIGH
EOP-002-2	R6.2.	Deploying all available operating reserve.	HIGH
EOP-002-2	R6.3.	Interrupting interruptible load and exports.	HIGH
EOP-002-2	R6.4.	Requesting emergency assistance from other Balancing Authorities.	HIGH
EOP-002-2	R6.5.	Declaring an Energy Emergency through its Reliability Coordinator; and	HIGH
EOP-002-2	R6.6.	Reducing load, through procedures such as public appeals, voltage reductions, curtailing interruptible loads and firm loads.	HIGH
EOP-002-2	R7.	Once the Balancing Authority has exhausted the steps listed in Requirement 6, or if these steps cannot be completed in sufficient time to resolve the emergency condition, the Balancing Authority shall:	HIGH
EOP-002-2	R7.1.	Manually shed firm load without delay to return its ACE to zero; and	HIGH
EOP-002-2	R7.2.	Request the Reliability Coordinator to declare an Energy Emergency Alert in accordance with Attachment 1-EOP-002-0 "Energy Emergency Alert Levels."	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
EOP-002-2	R8.	A Reliability Coordinator that has any Balancing Authority within its Reliability Coordinator area experiencing a potential or actual Energy Emergency shall initiate an Energy Emergency Alert as detailed in Attachment 1-EOP-002-0 "Energy Emergency Alert Levels." The Reliability Coordinator shall act to mitigate the emergency condition, including a request for emergency assistance if required.	HIGH
EOP-002-2	R9.	When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources) as permitted in its transmission tariff (See Attachment 1-IRO-006-0 "Transmission Loading Relief Procedure" for explanation of Transmission Service Priorities):	HIGH
EOP-002-2	R9.1.	The deficient Load-Serving Entity shall request its Reliability Coordinator to initiate an Energy Emergency Alert in accordance with Attachment 1-EOP-002-0.	HIGH
EOP-002-2	R9.2.	The Reliability Coordinator shall submit the report to NERC for posting on the NERC Website, noting the expected total MW that may have its transmission service priority changed.	HIGH
EOP-002-2	R9.3.	The Reliability Coordinator shall use EEA 1 to forecast the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to Priority 7.	LOWER
EOP-002-2	R9.4.	The Reliability Coordinator shall use EEA 2 to announce the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to Priority 7.	LOWER
EOP-003-1	R1.	After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.	HIGH
EOP-003-1	R2.	Each Transmission Operator and Balancing Authority shall establish plans for automatic load shedding for underfrequency or undervoltage conditions.	HIGH
EOP-003-1	R3.	Each Transmission Operator and Balancing Authority shall coordinate load shedding plans among other interconnected Transmission Operators and Balancing Authorities.	HIGH
EOP-003-1	R4.	A Transmission Operator or Balancing Authority shall consider one or more of these factors in designing an automatic load shedding scheme: frequency, rate of frequency decay, voltage level, rate of voltage decay, or power flow levels.	HIGH
EOP-003-1	R5.	A Transmission Operator or Balancing Authority shall implement load shedding in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
EOP-003-1	R6.	After a Transmission Operator or Balancing Authority Area separates from the Interconnection, if there is insufficient generating capacity to restore system frequency following automatic underfrequency load shedding, the Transmission Operator or Balancing Authority shall shed additional load.	HIGH
EOP-003-1	R7.	The Transmission Operator and Balancing Authority shall coordinate automatic load shedding throughout their areas with underfrequency isolation of generating units, tripping of shunt capacitors, and other automatic actions that will occur under abnormal frequency, voltage, or power flow conditions.	HIGH
EOP-003-1	R8.	Each Transmission Operator or Balancing Authority shall have plans for operator-controlled manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be capable of implementing the load shedding in a timeframe adequate for responding to the emergency.	HIGH
EOP-004-1	R1.	Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	LOWER
EOP-004-1	R2.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	MEDIUM
EOP-004-1	R3.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.	LOWER
EOP-004-1	R3.1.	The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.	LOWER
EOP-004-1	R3.2.	Applicable reporting forms are provided in Attachments 022-1 and 022-2.	<blank>

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
EOP-004-1	R3.3.	Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	LOWER
EOP-004-1	R3.4.	If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.	LOWER
EOP-004-1	R4.	When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	LOWER
EOP-004-1	R5.	The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.	LOWER
EOP-005-1	R1.	Each Transmission Operator shall have a restoration plan to reestablish its electric system in a stable and orderly manner in the event of a partial or total shutdown of its system, including necessary operating instructions and procedures to cover emergency conditions, and the loss of vital telecommunications channels. Each Transmission Operator shall include the applicable elements listed in Attachment 1-EOP-005 in developing a restoration plan.	MEDIUM
EOP-005-1	R2.	Each Transmission Operator shall review and update its restoration plan at least annually and whenever it makes changes in the power system network, and shall correct deficiencies found during the simulated restoration exercises.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
EOP-005-1	R3.	Each Transmission Operator shall develop restoration plans with a priority of restoring the integrity of the Interconnection.	MEDIUM
EOP-005-1	R4.	Each Transmission Operator shall coordinate its restoration plans with the Generator Owners and Balancing Authorities within its area, its Reliability Coordinator, and neighboring Transmission Operators and Balancing Authorities.	MEDIUM
EOP-005-1	R5.	Each Transmission Operator and Balancing Authority shall periodically test its telecommunication facilities needed to implement the restoration plan.	MEDIUM
EOP-005-1	R6.	Each Transmission Operator and Balancing Authority shall train its operating personnel in the implementation of the restoration plan. Such training shall include simulated exercises, if practicable.	HIGH
EOP-005-1	R7.	Each Transmission Operator and Balancing Authority shall verify the restoration procedure by actual testing or by simulation.	HIGH
EOP-005-1	R8.	Each Transmission Operator shall verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan requirements for the Transmission Operator's area.	HIGH
EOP-005-1	R9.	The Transmission Operator shall document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started and shall provide this documentation for review by the Regional Reliability Organization upon request. Such documentation may include Cranking Path diagrams.	MEDIUM
EOP-005-1	R10.	The Transmission Operator shall demonstrate, through simulation or testing, that the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	MEDIUM
EOP-005-1	R10.1.	The Transmission Operator shall perform this simulation or testing at least once every five years.	MEDIUM
EOP-005-1	R11.	Following a disturbance in which one or more areas of the Bulk Electric System become isolated or blacked out, the affected Transmission Operators and Balancing Authorities shall begin immediately to return the Bulk Electric System to normal.	HIGH
EOP-005-1	R11.1.	The affected Transmission Operators and Balancing Authorities shall work in conjunction with their Reliability Coordinator(s) to determine the extent and condition of the isolated area(s).	MEDIUM
EOP-005-1	R11.2.	The affected Transmission Operators and Balancing Authorities shall take the necessary actions to restore Bulk Electric System frequency to normal, including adjusting generation, placing additional generators on line, or load shedding.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
EOP-005-1	R11.3.	The affected Balancing Authorities, working with their Reliability Coordinator(s), shall immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments as needed to facilitate the restoration. The affected Balancing Authorities shall make all attempts to maintain the adjusted Interchange Schedules, whether generation control is manual or automatic.	HIGH
EOP-005-1	R11.4.	The affected Transmission Operators shall give high priority to restoration of off-site power to nuclear stations.	HIGH
EOP-005-1	R11.5.	The affected Transmission Operators may resynchronize the isolated area(s) with the surrounding area(s) when the following conditions are met:	MEDIUM
EOP-005-1	R11.5.1.	Voltage, frequency, and phase angle permit.	HIGH
EOP-005-1	R11.5.2.	The size of the area being reconnected and the capacity of the transmission lines effecting the reconnection and the number of synchronizing points across the system are considered.	HIGH
EOP-005-1	R11.5.3.	Reliability Coordinator(s) and adjacent areas are notified and Reliability Coordinator approval is given.	MEDIUM
EOP-005-1	R11.5.4.	Load is shed in neighboring areas, if required, to permit successful interconnected system restoration.	HIGH
EOP-006-1	R1.	Each Reliability Coordinator shall be aware of the restoration plan of each Transmission Operator in its Reliability Coordinator Area in accordance with NERC and regional requirements.	MEDIUM
EOP-006-1	R2.	The Reliability Coordinator shall monitor restoration progress and coordinate any needed assistance.	HIGH
EOP-006-1	R3.	The Reliability Coordinator shall have a Reliability Coordinator Area restoration plan that provides coordination between individual Transmission Operator restoration plans and that ensures reliability is maintained during system restoration events.	MEDIUM
EOP-006-1	R4.	The Reliability Coordinator shall serve as the primary contact for disseminating information regarding restoration to neighboring Reliability Coordinators and Transmission Operators or Balancing Authorities not immediately involved in restoration.	MEDIUM
EOP-006-1	R5.	Reliability Coordinators shall approve, communicate, and coordinate the re-synchronizing of major system islands or synchronizing points so as not to cause a Burden on adjacent Transmission Operator, Balancing Authority, or Reliability Coordinator Areas.	HIGH
EOP-006-1	R6.	The Reliability Coordinator shall take actions to restore normal operations once an operating emergency has been mitigated in accordance with its restoration plan.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
EOP-008-0	R1.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have a plan to continue reliability operations in the event its control center becomes inoperable. The contingency plan must meet the following requirements:	HIGH
EOP-008-0	R1.1.	The contingency plan shall not rely on data or voice communication from the primary control facility to be viable.	MEDIUM
EOP-008-0	R1.2.	The plan shall include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.	MEDIUM
EOP-008-0	R1.3.	The contingency plan must address monitoring and control of critical transmission facilities, generation control, voltage control, time and frequency control, control of critical substation devices, and logging of significant power system events. The plan shall list the critical facilities.	MEDIUM
EOP-008-0	R1.4.	The plan shall include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.	HIGH
EOP-008-0	R1.5.	The plan shall include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.	MEDIUM
EOP-008-0	R1.6.	The plan shall include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.	MEDIUM
EOP-008-0	R1.7.	The plan shall be reviewed and updated annually.	MEDIUM
EOP-008-0	R1.8.	Interim provisions must be included if it is expected to take more than one hour to implement the contingency plan for loss of primary control facility.	MEDIUM
EOP-009-0	R1.	The Generator Operator of each blackstart generating unit shall test the startup and operation of each system blackstart generating unit identified in the BCP as required in the Regional BCP (Reliability Standard EOP-007-0_R1). Testing records shall include the dates of the tests, the duration of the tests, and an indication of whether the tests met Regional BCP requirements.	MEDIUM
EOP-009-0	R2.	The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-001-0	R1.	The Transmission Owner shall document, maintain, and publish facility connection requirements to ensure compliance with NERC Reliability Standards and applicable Regional Reliability Organization, subregional, Power Pool, and individual Transmission Owner planning criteria and facility connection requirements. The Transmission Owner's facility connection requirements shall address connection requirements for:	MEDIUM
FAC-001-0	R1.1.	Generation facilities,	MEDIUM
FAC-001-0	R1.2.	Transmission facilities, and	MEDIUM
FAC-001-0	R1.3.	End-user facilities	MEDIUM
FAC-001-0	R2.	The Transmission Owner's facility connection requirements shall address, but are not limited to, the following items:	MEDIUM
FAC-001-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	MEDIUM
FAC-001-0	R2.1.1.	Procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems.	MEDIUM
FAC-001-0	R2.1.2.	Procedures for notification of new or modified facilities to others (those responsible for the reliability of the interconnected transmission systems) as soon as feasible.	MEDIUM
FAC-001-0	R2.1.3.	Voltage level and MW and MVAR capacity or demand at point of connection.	MEDIUM
FAC-001-0	R2.1.4.	Breaker duty and surge protection.	MEDIUM
FAC-001-0	R2.1.5.	System protection and coordination.	MEDIUM
FAC-001-0	R2.1.6.	Metering and telecommunications.	MEDIUM
FAC-001-0	R2.1.7.	Grounding and safety issues.	MEDIUM
FAC-001-0	R2.1.8.	Insulation and insulation coordination.	MEDIUM
FAC-001-0	R2.1.9.	Voltage, Reactive Power, and power factor control.	MEDIUM
FAC-001-0	R2.1.10.	Power quality impacts.	MEDIUM
FAC-001-0	R2.1.11.	Equipment Ratings.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-001-0	R2.1.12.	Synchronizing of facilities.	MEDIUM
FAC-001-0	R2.1.13.	Maintenance coordination.	MEDIUM
FAC-001-0	R2.1.14.	Operational issues (abnormal frequency and voltages).	MEDIUM
FAC-001-0	R2.1.15.	Inspection requirements for existing or new facilities.	MEDIUM
FAC-001-0	R2.1.16.	Communications and procedures during normal and emergency operating conditions.	MEDIUM
FAC-001-0	R3.	The Transmission Owner shall maintain and update its facility connection requirements as required. The Transmission Owner shall make documentation of these requirements available to the users of the transmission system, the Regional Reliability Organization, and NERC on request (five business days).	MEDIUM
FAC-002-0	R1.	The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:	MEDIUM
FAC-002-0	R1.1.	Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.	MEDIUM
FAC-002-0	R1.2.	Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.	MEDIUM
FAC-002-0	R1.3.	Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.	MEDIUM
FAC-002-0	R1.4.	Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance in accordance with Reliability Standard TPL-001-0.	MEDIUM
FAC-002-0	R1.5.	Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.	MEDIUM
FAC-002-0	R2.	The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) Regional Reliability Organization(s) and NERC on request (within 30 calendar days).	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-003-1	R1.	The Transmission owner shall prepare, and keep current, a formal transmission vegetation management (TVM). The TVMP shall include the Transmission Owner's objectives, practices, approved procedures, and work Specifications. 1. ANSI A300, Tree Care Operations – Tree, Shrub, and Other Woody Plant Maintenance – Standard Practices, while not a requirement of this standard, is considered to be an industry best practice.	HIGH
FAC-003-1	R1.1.	The TVMP shall define a schedule for and the type (aerial, ground) of ROW vegetation inspections. This schedule should be flexible enough to adjust for changing conditions. The inspection schedule shall be based on the anticipated growth of vegetation and any other environmental or operational factors that could impact the relationship of vegetation to the Transmission Owner's transmission lines.	HIGH
FAC-003-1	R1.2.	The Transmission Owner, in the TVMP, shall identify and document clearances between vegetation and any overhead, ungrounded supply conductors, taking into consideration transmission line voltage, the effects of ambient temperature on conductor sag under maximum design loading, and the effects of wind velocities on conductor sway. Specifically, the Transmission Owner shall establish clearances to be achieved at the time of vegetation management work identified herein as Clearance 1, and shall also establish and maintain a set of clearances identified herein as Clearance 2 to prevent flashover between vegetation and overhead ungrounded supply conductors.	HIGH
FAC-003-1	R1.2.1.	Clearance 1 — The Transmission Owner shall determine and document appropriate clearance distances to be achieved at the time of transmission vegetation management work based upon local conditions and the expected time frame in which the Transmission Owner plans to return for future vegetation management work. Local conditions may include, but are not limited to: operating voltage, appropriate vegetation management techniques, fire risk, reasonably anticipated tree and conductor movement, species types and growth rates, species failure characteristics, local climate and rainfall patterns, line terrain and elevation, location of the vegetation within the span, and worker approach distance requirements. Clearance 1 distances shall be greater than those defined by Clearance 2 below.	HIGH
FAC-003-1	R1.2.2.	Clearance 2 — The Transmission Owner shall determine and document specific radial clearances to be maintained between vegetation and conductors under all rated electrical operating conditions. These minimum clearance distances are necessary to prevent flashover between vegetation and conductors and will vary due to such factors as altitude and operating voltage. These Transmission Owner-specific minimum clearance distances shall be no less than those set forth in the Institute of Electrical and Electronics Engineers (IEEE) Standard 516-2003 (<i>Guide for Maintenance Methods on Energized Power Lines</i>) and as specified in its Section 4.2.2.3, Minimum Air Insulation Distances without Tools in the Air Gap.	HIGH
FAC-003-1	R1.2.2.1.	Where transmission system transient overvoltage factors are not known, clearances shall be derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-003-1	R1.2.2.2.	Where transmission system transient overvoltage factors are known, clearances shall be derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.	HIGH
FAC-003-1	R1.3.	All personnel directly involved in the design and implementation of the TVMP shall hold appropriate qualifications and training, as defined by the Transmission Owner, to perform their duties.	HIGH
FAC-003-1	R1.4.	Each Transmission Owner shall develop mitigation measures to achieve sufficient clearances for the protection of the transmission facilities when it identifies locations on the ROW where the Transmission Owner is restricted from attaining the clearances specified in Requirement 1.2.1.	HIGH
FAC-003-1	R1.5.	Each Transmission Owner shall establish and document a process for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage. This is so that action (temporary reduction in line rating, switching line out of service, etc.) may be taken until the threat is relieved.	HIGH
FAC-003-1	R2.	The Transmission Owner shall create and implement an annual plan for vegetation management work to ensure the reliability of the system. The plan shall describe the methods used, such as manual clearing, mechanical clearing, herbicide treatment, or other actions. The plan should be flexible enough to adjust to changing conditions, taking into consideration anticipated growth of vegetation and all other environmental factors that may have an impact on the reliability of the transmission systems. Adjustments to the plan shall be documented as they occur. The plan should take into consideration the time required to obtain permissions or permits from landowners or regulatory authorities. Each Transmission Owner shall have systems and procedures for documenting and tracking the planned vegetation management work and ensuring that the vegetation management work was completed according to work specifications.	HIGH
FAC-003-1	R3.	The Transmission Owner shall report quarterly to its RRO, or the RRO's designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation.	LOWER
FAC-003-1	R3.1.	Multiple sustained outages on an individual line, if caused by the same vegetation, shall be reported as one outage regardless of the actual number of outages within a 24-hour period.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-003-1	R3.2.	The Transmission Owner is not required to report to the RRO, or the RRO's designee, certain sustained transmission line outages caused by vegetation: (1) Vegetation-related outages that result from vegetation falling into lines from outside the ROW that result from natural disasters shall not be considered reportable (examples of disasters that could create non-reportable outages include, but are not limited to, earthquakes, fires, tornados, hurricanes, landslides, wind shear, major storms as defined either by the Transmission Owner or an applicable regulatory body, ice storms, and floods), and (2) Vegetation-related outages due to human or animal activity shall not be considered reportable (examples of human or animal activity that could cause a non-reportable outage include, but are not limited to, logging, animal severing tree, vehicle contact with tree, arboricultural activities or horticultural or agricultural activities, or removal or digging of vegetation).	LOWER
FAC-003-1	R3.3.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, shall include at a minimum: the name of the circuit(s) outaged, the date, time and duration of the outage; a description of the cause of the outage; other pertinent comments; and any countermeasures taken by the Transmission Owner.	LOWER
FAC-003-1	R3.4.	An outage shall be categorized as one of the following:	LOWER
FAC-003-1	R3.4.1.	Category 1 — Grow-ins: Outages caused by vegetation growing into lines from vegetation inside and/or outside of the ROW;	LOWER
FAC-003-1	R3.4.2.	Category 2 — Fall-ins: Outages caused by vegetation falling into lines from inside the ROW;	LOWER
FAC-003-1	R3.4.3.	Category 3 — Fall-ins: Outages caused by vegetation falling into lines from outside the ROW.	LOWER
FAC-003-1	R4.	The RRO shall report the outage information provided to it by Transmission Owner's, as required by Requirement 3, quarterly to NERC, as well as any actions taken by the RRO as a result of any of the reported outages.	LOWER
FAC-008-1	R1.	The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:	LOWER
FAC-008-1	R1.1.	A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.	MEDIUM
FAC-008-1	R1.2.	The method by which the Rating (of major BES equipment that comprises a Facility) is determined.	MEDIUM
FAC-008-1	R1.2.1.	The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-008-1	R1.2.2.	The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.	MEDIUM
FAC-008-1	R1.3.	Consideration of the following:	LOWER
FAC-008-1	R1.3.1.	Ratings provided by equipment manufacturers.	MEDIUM
FAC-008-1	R1.3.2.	Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).	MEDIUM
FAC-008-1	R1.3.3.	Ambient conditions.	MEDIUM
FAC-008-1	R1.3.4.	Operating limitations.	MEDIUM
FAC-008-1	R1.3.5.	Other assumptions.	LOWER
FAC-008-1	R2.	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.	LOWER
FAC-008-1	R3.	If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.	LOWER
FAC-009-1	R1.	The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology.	MEDIUM
FAC-009-1	R2.	The Transmission Owner and Generator Owner shall each provide Facility Ratings for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities to its associated Reliability Coordinator(s), Planning Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities.	MEDIUM
FAC-010-1	R1.	The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:	LOWER
FAC-010-1	R1.1.	Be applicable for developing SOLs used in the planning horizon.	LOWER
FAC-010-1	R1.2.	State that SOLs shall not exceed associated Facility Ratings.	LOWER
FAC-010-1	R1.3.	Include a description of how to identify the subset of SOLs that qualify as IROLs.	LOWER
FAC-010-1	R2.	The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:	REMOVE

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-010-1	R2.1.	In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.	HIGH
FAC-010-1	R2.2.	Following the single Contingencies ¹ identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading Outages or uncontrolled separation shall not occur.	HIGH
FAC-010-1	R2.2.1.	Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.	MEDIUM
FAC-010-1	R2.2.2.	Loss of any generator, line, transformer, or shunt device without a Fault.	MEDIUM
FAC-010-1	R2.2.3.	Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.	MEDIUM
FAC-010-1	R2.3.	Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:	MEDIUM
FAC-010-1	R2.3.1.	Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.	MEDIUM
FAC-010-1	R2.3.2.	System reconfiguration through manual or automatic control or protection actions.	MEDIUM
FAC-010-1	R2.3.3.	To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.	MEDIUM
FAC-010-1	R2.4.	Starting with all facilities in service and following any of the multiple Contingencies identified in Reliability Standard TPL-003 the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading Outages or uncontrolled separation shall not occur.	MEDIUM
FAC-010-1	R2.5.	In determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2, the following shall be acceptable:	MEDIUM
FAC-010-1	R2.5.1.	Planned or controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers	MEDIUM
FAC-010-1	R3.	The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	LOWER
FAC-010-1	R3.1.	Study model (must include at least the entire Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).	LOWER
FAC-010-1	R3.2.	Selection of applicable Contingencies.	LOWER
FAC-010-1	R3.3.	Level of detail of system models used to determine SOLs.	LOWER
FAC-010-1	R3.4.	Allowed uses of Special Protection Systems or Remedial Action Plans.	MEDIUM
FAC-010-1	R3.5.	Anticipated transmission system configuration, generation dispatch and Load level.	LOWER
FAC-010-1	R3.6.	Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL Tv.	MEDIUM
FAC-010-1	R4.	The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-010-1	R4.1.	Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.	LOWER
FAC-010-1	R4.2.	Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.	LOWER
FAC-010-1	R4.3.	Each Transmission Planner that works in the Planning Authority's Planning Authority Area.	LOWER
FAC-010-1	R5.	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	LOWER
FAC-011-1	R1.	The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:	LOWER
FAC-011-1	R1.1.	Be applicable for developing SOLs used in the operations horizon.	LOWER
FAC-011-1	R1.2.	State that SOLs shall not exceed associated Facility Ratings.	LOWER
FAC-011-1	R1.3.	Include a description of how to identify the subset of SOLs that qualify as IROLs	LOWER
FAC-011-1	R2.	The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:	REMOVE
FAC-011-1	R2.1.	In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.	HIGH
FAC-011-1	R2.2.	Following the single Contingencies1 identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading Outages or uncontrolled separation shall not occur.	HIGH
FAC-011-1	R2.2.1.	Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.	MEDIUM
FAC-011-1	R2.2.2.	Loss of any generator, line, transformer, or shunt device without a Fault.	MEDIUM
FAC-011-1	R2.2.3.	Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.	MEDIUM
FAC-011-1	R2.3.	In determining the system's response to a single Contingency, the following shall be acceptable:	MEDIUM
FAC-011-1	R2.3.1.	Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.	MEDIUM
FAC-011-1	R2.3.2.	Interruption of other network customers, only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or, if the real-time operating conditions are more adverse than anticipated in the corresponding studies, e.g., load greater than studied.	MEDIUM
FAC-011-1	R2.3.3.	System reconfiguration through manual or automatic control or protection actions.	MEDIUM
FAC-011-1	R2.4.	To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.	MEDIUM
FAC-011-1	R3.	The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-011-1	R3.1.	Study model (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)	MEDIUM
FAC-011-1	R3.2.	Selection of applicable Contingencies	MEDIUM
FAC-011-1	R3.3.	A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.	MEDIUM
FAC-011-1	R3.3.1.	This process shall address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple contingencies.	
FAC-011-1	R3.4.	Level of detail of system models used to determine SOLs.	LOWER
FAC-011-1	R3.5.	Allowed uses of Special Protection Systems or Remedial Action Plans.	MEDIUM
FAC-011-1	R3.6.	Anticipated transmission system configuration, generation dispatch and Load level	MEDIUM
FAC-011-1	R3.7.	Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL Tv.	MEDIUM
FAC-011-1	R4.	The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:	LOWER
FAC-011-1	R4.1.	Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.	LOWER
FAC-011-1	R4.2.	Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.	LOWER
FAC-011-1	R4.3.	Each Transmission Operator that operates in the Reliability Coordinator Area.	LOWER
FAC-011-1	R5.	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	LOWER
FAC-013-1	R1.	The Reliability Coordinator and Planning Authority shall each establish a set of inter-regional and intra-regional Transfer Capabilities that is consistent with its current Transfer Capability Methodology.	MEDIUM
FAC-013-1	R2.	The Reliability Coordinator and Planning Authority shall each provide its inter-regional and intra-regional Transfer Capabilities to those entities that have a reliability-related need for such Transfer Capabilities and make a written request that includes a schedule for delivery of such Transfer Capabilities as follows:	MEDIUM
FAC-013-1	R2.1.	The Reliability Coordinator shall provide its Transfer Capabilities to its associated Regional Reliability Organization(s), to its adjacent Reliability Coordinators, and to the Transmission Operators, Transmission Service Providers and Planning Authorities that work in its Reliability Coordinator Area.	MEDIUM
FAC-013-1	R2.2.	The Planning Authority shall provide its Transfer Capabilities to its associated Reliability Coordinator(s) and Regional Reliability Organization(s), and to the Transmission Planners and Transmission Service Provider(s) that work in its Planning Authority Area.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-014-1	R1.	The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.	MEDIUM
FAC-014-1	R2.	The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology.	MEDIUM
FAC-014-1	R3.	The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology.	MEDIUM
FAC-014-1	R4.	The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology.	MEDIUM
FAC-014-1	R5.	The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows:	HIGH
FAC-014-1	R5.1.	The Reliability Coordinator shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Reliability Coordinators and Reliability Coordinators who indicate a reliability-related need for those limits, and to the Transmission Operators, Transmission Planners, Transmission Service Providers and Planning Authorities within its Reliability Coordinator Area. For each IROL, the Reliability Coordinator shall provide the following supporting information:	HIGH
FAC-014-1	R5.1.1.	Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL.	MEDIUM
FAC-014-1	R5.1.2.	The value of the IROL and its associated Tv.	MEDIUM
FAC-014-1	R5.1.3.	The associated Contingency(ies).	MEDIUM
FAC-014-1	R5.1.4.	The type of limitation represented by the IROL (e.g., voltage collapse, angular stability).	MEDIUM
FAC-014-1	R5.2.	The Transmission Operator shall provide any SOLs it developed to its Reliability Coordinator and to the Transmission Service Providers that share its portion of the Reliability Coordinator Area.	MEDIUM
FAC-014-1	R5.3.	The Planning Authority shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Planning Authorities, and to Transmission Planners, Transmission Service Providers, Transmission Operators and Reliability Coordinators that work within its Planning Authority Area.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
FAC-014-1	R5.4.	The Transmission Planner shall provide its SOLs (including the subset of SOLs that are IROLs) to its Planning Authority, Reliability Coordinators, Transmission Operators, and Transmission Service Providers that work within its Transmission Planning Area and to adjacent Transmission Planners.	MEDIUM
FAC-014-1	R6.	The Planning Authority shall identify the subset of multiple contingencies (if any), from Reliability Standard TPL-003 which result in stability limits.	MEDIUM
FAC-014-1	R6.1.	The Planning Authority shall provide this list of multiple contingencies and the associated stability limits to the Reliability Coordinators that monitor the facilities associated with these contingencies and limits.	MEDIUM
FAC-014-1	R6.2.	If the Planning Authority does not identify any stability-related multiple contingencies, the Planning Authority shall so notify the Reliability Coordinator.	MEDIUM
INT-001-3	R1.	The Load-Serving, Purchasing-Selling Entity shall ensure that Arranged Interchange is submitted to the Interchange Authority for:	LOWER
INT-001-3	R1.1.	All Dynamic Schedules at the expected average MW profile for each hour.	LOWER
INT-001-3	R2.	The Sink Balancing Authority shall ensure that Arranged Interchange is submitted to the Interchange Authority:	LOWER
INT-001-3	R2.1.	If a Purchasing-Selling Entity is not involved in the Interchange, such as delivery from a jointly owned generator.	LOWER
INT-001-3	R2.2.	For each bilateral Inadvertent Interchange payback.	LOWER
INT-003-2	R1.	Each Receiving Balancing Authority shall confirm Interchange Schedules with the Sending Balancing Authority prior to implementation in the Balancing Authority's ACE equation.	MEDIUM
INT-003-2	R1.1.	The Sending Balancing Authority and Receiving Balancing Authority shall agree on Interchange as received from the Interchange Authority, including:	LOWER
INT-003-2	R1.1.1.	Interchange Schedule start and end time.	LOWER
INT-003-2	R1.1.2.	Energy profile.	LOWER
INT-003-2	R1.2.	If a high voltage direct current (HVDC) tie is on the Scheduling Path, then the Sending Balancing Authorities and Receiving Balancing Authorities shall coordinate the Interchange Schedule with the Transmission Operator of the HVDC tie.	MEDIUM
INT-004-2	R1.	At such time as the reliability event allows for the reloading of the transaction, the entity that initiated the curtailment shall release the limit on the Interchange Transaction tag to allow reloading the transaction and shall communicate the release of the limit to the Sink Balancing Authority.	LOWER
INT-004-2	R2.	The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs:	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
INT-004-2	R2.1.	The average energy profile in an hour is greater than 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +10%.	LOWER
INT-004-2	R2.2.	The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +25 megawatt-hours.	LOWER
INT-004-2	R2.3.	A Reliability Coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons.	LOWER
INT-005-3	R1.	Prior to the expiration of the time period defined in the timing requirements tables in this standard, Column A, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment to all reliability entities involved in the Interchange.	MEDIUM
INT-005-3	R1.1.	When a Balancing Authority or Reliability Coordinator initiates a Curtailment to Confirmed or Implemented Interchange for reliability, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment only to the Source Balancing Authority and the Sink Balancing Authority.	MEDIUM
INT-006-3	R1.	Prior to the expiration of the reliability assessment period defined in the timing requirements tables in this standard, Column B, the Balancing Authority and Transmission Service Provider shall respond to each On-time Request for Interchange (RFI), and to each Emergency RFI and Reliability Adjustment RFI from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	LOWER
INT-006-3	R1.1.	Each involved Balancing Authority shall evaluate the Arranged Interchange with respect to:	LOWER
INT-006-3	R1.1.1.	Energy profile (ability to support the magnitude of the Interchange).	LOWER
INT-006-3	R1.1.2.	Ramp (ability of generation maneuverability to accommodate).	LOWER
INT-006-3	R1.1.3.	Scheduling path (proper connectivity of Adjacent Balancing Authorities).	LOWER
INT-006-3	R1.2.	Each involved Transmission Service Provider shall confirm that the transmission service arrangements associated with the Arranged Interchange have adjacent Transmission Service Provider connectivity, are valid and prevailing transmission system limits will not be violated.	LOWER
INT-007-1	R1.	The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:	LOWER
INT-007-1	R1.1.	Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).	LOWER
INT-007-1	R1.2.	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.	LOWER
INT-007-1	R1.3.	The following are defined:	LOWER
INT-007-1	R1.3.1.	Generation source and load sink.	LOWER
INT-007-1	R1.3.2.	Megawatt profile.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
INT-007-1	R1.3.3.	Ramp start and stop times.	LOWER
INT-007-1	R1.3.4.	Interchange duration.	LOWER
INT-007-1	R1.4.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.	LOWER
INT-008-3	R1.	Prior to the expiration of the time period defined in the Timing Table, Column C, the Interchange Authority shall distribute to all Balancing Authorities (including Balancing Authorities on both sides of a direct current tie), Transmission Service Providers and Purchasing-Selling Entities involved in the Arranged Interchange whether or not the Arranged Interchange has transitioned to a Confirmed Interchange.	LOWER
INT-008-3	R1.1.	For Confirmed Interchange, the Interchange Authority shall also communicate:	LOWER
INT-008-3	R1.1.1.	Start and stop times, ramps, and megawatt profile to Balancing Authorities.	LOWER
INT-008-3	R1.1.2.	Necessary Interchange information to NERC-identified reliability analysis services.	LOWER
INT-009-1	R1.	The Balancing Authority shall implement Confirmed Interchange as received from the Interchange Authority.	MEDIUM
INT-010-1	R1.	The Balancing Authority that experiences a loss of resources covered by an energy sharing agreement shall ensure that a request for an Arranged Interchange is submitted with a start time no more than 60 minutes beyond the resource loss. If the use of the energy sharing agreement does not exceed 60 minutes from the time of the resource loss, no request for Arranged Interchange is required.	LOWER
INT-010-1	R2.	For a modification to an existing Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit the modified Arranged Interchange reflecting that modification within 60 minutes of the initiation of the event.	LOWER
INT-010-1	R3.	For a new Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit an Arranged Interchange reflecting that Interchange schedule within 60 minutes of the initiation of the event.	LOWER
IRO-001-1.1	R1.	Each Regional Reliability Organization, subregion, or interregional coordinating group shall establish one or more Reliability Coordinators to continuously assess transmission reliability and coordinate emergency operations among the operating entities within the region and across the regional boundaries.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-001-1.1	R2.	The Reliability Coordinator shall comply with a regional reliability plan approved by the NERC Operating Committee.	HIGH
IRO-001-1.1	R3.	The Reliability Coordinator shall have clear decision-making authority to act and to direct actions to be taken by Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities within its Reliability Coordinator Area to preserve the integrity and reliability of the Bulk Electric System. These actions shall be taken without delay, but no longer than 30 minutes.	HIGH
IRO-001-1.1	R4.	Reliability Coordinators that delegate tasks to other entities shall have formal operating agreements with each entity to which tasks are delegated. The Reliability Coordinator shall verify that all delegated tasks are understood, communicated, and addressed within its Reliability Coordinator Area. All responsibilities for complying with NERC and regional standards applicable to Reliability Coordinators shall remain with the Reliability Coordinator.	MEDIUM
IRO-001-1.1	R5.	The Reliability Coordinator shall list within its reliability plan all entities to which the Reliability Coordinator has delegated required tasks.	LOWER
IRO-001-1.1	R6.	The Reliability Coordinator shall verify that all delegated tasks are carried out by NERC-certified Reliability Coordinator operating personnel.	MEDIUM
IRO-001-1.1	R7.	The Reliability Coordinator shall have clear, comprehensive coordination agreements with adjacent Reliability Coordinators to ensure that System Operating Limit or Interconnection Reliability Operating Limit violation mitigation requiring actions in adjacent Reliability Coordinator Areas are coordinated.	HIGH
IRO-001-1.1	R8.	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.	HIGH
IRO-001-1.1	R9.	The Reliability Coordinator shall act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of any other entity.	HIGH
IRO-002-1	R1.	Each Reliability Coordinator shall have adequate communications facilities (voice and data links) to appropriate entities within its Reliability Coordinator Area. These communications facilities shall be staffed and available to act in addressing a real-time emergency condition.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-002-1	R2.	Each Reliability Coordinator shall determine the data requirements to support its reliability coordination tasks and shall request such data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities, or adjacent Reliability Coordinators.	MEDIUM
IRO-002-1	R3.	Each Reliability Coordinator – or its Transmission Operators and Balancing Authorities – shall provide, or arrange provisions for, data exchange to other Reliability Coordinators or Transmission Operators and Balancing Authorities via a secure network.	MEDIUM
IRO-002-1	R4.	Each Reliability Coordinator shall have multi-directional communications capabilities with its Transmission Operators and Balancing Authorities, and with neighboring Reliability Coordinators, for both voice and data exchange as required to meet reliability needs of the Interconnection.	HIGH
IRO-002-1	R5.	Each Reliability Coordinator shall have detailed real-time monitoring capability of its Reliability Coordinator Area and sufficient monitoring capability of its surrounding Reliability Coordinator Areas to ensure that potential or actual System Operating Limit or Interconnection Reliability Operating Limit violations are identified. Each Reliability Coordinator shall have monitoring systems that provide information that can be easily understood and interpreted by the Reliability Coordinator’s operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant and highly reliable infrastructure.	HIGH
IRO-002-1	R6.	Each Reliability Coordinator shall monitor Bulk Electric System elements (generators, transmission lines, buses, transformers, breakers, etc.) that could result in SOL or IROL violations within its Reliability Coordinator Area. Each Reliability Coordinator shall monitor both real and reactive power system flows, and operating reserves, and the status of Bulk Electric System elements that are or could be critical to SOLs and IROLs and system restoration requirements within its Reliability Coordinator Area.	HIGH
IRO-002-1	R7.	Each Reliability Coordinator shall have adequate analysis tools such as state estimation, pre- and post-contingency analysis capabilities (thermal, stability, and voltage), and wide-area overview displays.	HIGH
IRO-002-1	R8.	Each Reliability Coordinator shall continuously monitor its Reliability Coordinator Area. Each Reliability Coordinator shall have provisions for backup facilities that shall be exercised if the main monitoring system is unavailable. Each Reliability Coordinator shall ensure SOL and IROL monitoring and derivations continue if the main monitoring system is unavailable.	HIGH
IRO-002-1	R9.	Each Reliability Coordinator shall control its Reliability Coordinator analysis tools, including approvals for planned maintenance. Each Reliability Coordinator shall have procedures in place to mitigate the effects of analysis tool outages.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-003-2	R1.	Each Reliability Coordinator shall monitor all Bulk Electric System facilities, which may include sub-transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.	HIGH
IRO-003-2	R2.	Each Reliability Coordinator shall know the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation. Reliability Coordinators shall also know the status of any facilities that may be required to assist area restoration objectives.	HIGH
IRO-004-1	R1.	Each Reliability Coordinator shall conduct next-day reliability analyses for its Reliability Coordinator Area to ensure that the Bulk Electric System can be operated reliably in anticipated normal and Contingency event conditions. The Reliability Coordinator shall conduct Contingency analysis studies to identify potential interface and other SOL and IROL violations, including overloaded transmission lines and transformers, voltage and stability limits, etc.	HIGH
IRO-004-1	R2.	Each Reliability Coordinator shall pay particular attention to parallel flows to ensure one Reliability Coordinator Area does not place an unacceptable or undue Burden on an adjacent Reliability Coordinator Area.	HIGH
IRO-004-1	R3.	Each Reliability Coordinator shall, in conjunction with its Transmission Operators and Balancing Authorities, develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs.	HIGH
IRO-004-1	R4.	Each Transmission Operator, Balancing Authority, Transmission Owner, Generator Owner, Generator Operator, and Load-Serving Entity in the Reliability Coordinator Area shall provide information required for system studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions. This information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.	HIGH
IRO-004-1	R5.	Each Reliability Coordinator shall share the results of its system studies, when conditions warrant or upon request, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area. The Reliability Coordinator shall make study results available no later than 1500 Central Standard Time for the Eastern Interconnection and 1500 Pacific Standard Time for the Western Interconnection, unless circumstances warrant otherwise.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-004-1	R6.	If the results of these studies indicate potential SOL or IROL violations, the Reliability Coordinator shall direct its Transmission Operators, Balancing Authorities and Transmission Service Providers to take any necessary action the Reliability Coordinator deems appropriate to address the potential SOL or IROL violation.	HIGH
IRO-004-1	R7.	Each Transmission Operator, Balancing Authority, and Transmission Service Provider shall comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events.	HIGH
IRO-005-2	R1.	Each Reliability Coordinator shall monitor its Reliability Coordinator Area parameters, including but not limited to the following:	HIGH
IRO-005-2	R1.1.	Current status of Bulk Electric System elements (transmission or generation including critical auxiliaries such as Automatic Voltage Regulators and Special Protection Systems) and system loading.	HIGH
IRO-005-2	R1.2.	Current pre-contingency element conditions (voltage, thermal, or stability), including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.	HIGH
IRO-005-2	R1.3.	Current post-contingency element conditions (voltage, thermal, or stability), including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.	HIGH
IRO-005-2	R1.4.	System real and reactive reserves (actual versus required).	HIGH
IRO-005-2	R1.5.	Capacity and energy adequacy conditions.	HIGH
IRO-005-2	R1.6.	Current ACE for all its Balancing Authorities.	HIGH
IRO-005-2	R1.7.	Current local or Transmission Loading Relief procedures in effect.	HIGH
IRO-005-2	R1.8.	Planned generation dispatches.	HIGH
IRO-005-2	R1.9.	Planned transmission or generation outages.	HIGH
IRO-005-2	R1.10.	Contingency events.	HIGH
IRO-005-2	R2.	Each Reliability Coordinator shall be aware of all Interchange Transactions that wheel through, source, or sink in its Reliability Coordinator Area, and make that Interchange Transaction information available to all Reliability Coordinators in the Interconnection.	HIGH
IRO-005-2	R3.	As portions of the transmission system approach or exceed SOLs or IROLs, the Reliability Coordinator shall work with its Transmission Operators and Balancing Authorities to evaluate and assess any additional Interchange Schedules that would violate those limits. If a potential or actual IROL violation cannot be avoided through proactive intervention, the Reliability Coordinator shall initiate control actions or emergency procedures to relieve the violation without delay, and no longer than 30 minutes. The Reliability Coordinator shall ensure all resources, including load shedding, are available to address a potential or actual IROL violation.	HIGH
IRO-005-2	R4.	Each Reliability Coordinator shall monitor its Balancing Authorities' parameters to ensure that the required amount of operating reserves is provided and available as required to meet the Control Performance Standard and Disturbance Control Standard requirements. If necessary, the Reliability Coordinator shall direct the Balancing Authorities in the Reliability Coordinator Area to arrange for assistance from neighboring Balancing Authorities. The Reliability Coordinator shall issue Energy Emergency Alerts as needed and at the request of its Balancing Authorities and Load-Serving Entities.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-005-2	R5.	Each Reliability Coordinator shall identify the cause of any potential or actual SOL or IROL violations. The Reliability Coordinator shall initiate the control action or emergency procedure to relieve the potential or actual IROL violation without delay, and no longer than 30 minutes. The Reliability Coordinator shall be able to utilize all resources, including load shedding, to address an IROL violation.	HIGH
IRO-005-2	R6.	Each Reliability Coordinator shall ensure its Transmission Operators and Balancing Authorities are aware of Geo-Magnetic Disturbance (GMD) forecast information and assist as needed in the development of any required response plans.	HIGH
IRO-005-2	R7.	The Reliability Coordinator shall disseminate information within its Reliability Coordinator Area, as required.	HIGH
IRO-005-2	R8.	Each Reliability Coordinator shall monitor system frequency and its Balancing Authorities' performance and direct any necessary rebalancing to return to CPS and DCS compliance. The Transmission Operators and Balancing Authorities shall utilize all resources, including firm load shedding, as directed by its Reliability Coordinator to relieve the emergent condition.	HIGH
IRO-005-2	R9.	The Reliability Coordinator shall coordinate with Transmission Operators, Balancing Authorities, and Generator Operators as needed to develop and implement action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations. The Reliability Coordinator shall coordinate pending generation and transmission maintenance outages with Transmission Operators, Balancing Authorities, and Generator Operators as needed in both the real time and next-day reliability analysis timeframes.	HIGH
IRO-005-2	R10.	As necessary, the Reliability Coordinator shall assist the Balancing Authorities in its Reliability Coordinator Area in arranging for assistance from neighboring Reliability Coordinator Areas or Balancing Authorities.	HIGH
IRO-005-2	R11.	The Reliability Coordinator shall identify sources of large Area Control Errors that may be contributing to Frequency Error, Time Error, or Inadvertent Interchange and shall discuss corrective actions with the appropriate Balancing Authority. The Reliability Coordinator shall direct its Balancing Authority to comply with CPS and DCS.	HIGH
IRO-005-2	R12.	Whenever a Special Protection System that may have an inter-Balancing Authority, or inter-Transmission Operator impact (e.g., could potentially affect transmission flows resulting in a SOL or IROL violation) is armed, the Reliability Coordinators shall be aware of the impact of the operation of that Special Protection System on inter-area flows. The Transmission Operator shall immediately inform the Reliability Coordinator of the status of the Special Protection System including any degradation or potential failure to operate as expected.	HIGH
IRO-005-2	R13.	Each Reliability Coordinator shall ensure that all Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities operate to prevent the likelihood that a disturbance, action, or nonaction in its Reliability Coordinator Area will result in a SOL or IROL violation in another area of the Interconnection. In instances where there is a difference in derived limits, the Reliability Coordinator and its Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall always operate the Bulk Electric System to the most limiting parameter.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-005-2	R14.	Each Reliability Coordinator shall make known to Transmission Service Providers within its Reliability Coordinator Area, SOLs or IROLs within its wide-area view. The Transmission Service Providers shall respect these SOLs or IROLs in accordance with filed tariffs and regional Total Transfer Calculation and Available Transfer Calculation processes.	MEDIUM
IRO-005-2	R15.	Each Reliability Coordinator who foresees a transmission problem (such as an SOL or IROL violation, loss of reactive reserves, etc.) within its Reliability Coordinator Area shall issue an alert to all impacted Transmission Operators and Balancing Authorities in its Reliability Coordinator Area without delay. The receiving Reliability Coordinator shall disseminate this information to its impacted Transmission Operators and Balancing Authorities. The Reliability Coordinator shall notify all impacted Transmission Operators, Balancing Authorities, when the transmission problem has been mitigated.	HIGH
IRO-005-2	R16.	Each Reliability Coordinator shall confirm reliability assessment results and determine the effects within its own and adjacent Reliability Coordinator Areas. The Reliability Coordinator shall discuss options to mitigate potential or actual SOL or IROL violations and take actions as necessary to always act in the best interests of the Interconnection at all times.	HIGH
IRO-005-2	R17.	When an IROL or SOL is exceeded, the Reliability Coordinator shall evaluate the local and wide-area impacts, both real-time and post-contingency, and determine if the actions being taken are appropriate and sufficient to return the system to within IROL in thirty minutes. If the actions being taken are not appropriate or sufficient, the Reliability Coordinator shall direct the Transmission Operator, Balancing Authority, Generator Operator, or Load-Serving Entity to return the system to within IROL or SOL.	HIGH
IRO-006-4	R1.	A Reliability Coordinator experiencing a potential or actual SOL or IROL violation within its Reliability Coordinator Area shall, with its authority and at its discretion, select one or more procedures to provide transmission loading relief. These procedures can be a "local" (regional, interregional, or sub-regional) transmission loading relief procedure or one of the following Interconnection-wide procedures: [Time Horizon: Real-time Operations]	MEDIUM
IRO-006-4	R1.1.	The Interconnection-wide Transmission Loading Relief (TLR) procedure for use in the Eastern Interconnection provided in Attachment 1-IRO-006-4. The TLR procedure alone is an inappropriate and ineffective tool to mitigate an IROL violation due to the time required to implement the procedure. Other acceptable and more effective procedures to mitigate actual IROL violations include: reconfiguration, redispatch, or load shedding.	<blank>
IRO-006-4	R1.2.	The Interconnection-wide transmission loading relief procedure for use in the Western Interconnection is WECC-IRO-STD-006-0 provided at: ftp://www.nerc.com/pub/sys/all_updl/standards/rrs/IRO-STD-006-0_17Jan07.pdf .	<blank>
IRO-006-4	R1.3.	The Interconnection-wide transmission loading relief procedure for use in ERCOT is provided as Section 7 of the ERCOT Protocols, posted at: http://www.ercot.com/mktrules/protocols/current.html	<blank>

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-006-4	R2.	The Reliability Coordinator shall only use local transmission loading relief or congestion management procedures to which the Transmission Operator experiencing the potential or actual SOL or IROL violation is a party. [Time Horizon: Operations Planning]	LOWER
IRO-006-4	R3.	Each Reliability Coordinator with a relief obligation from an Interconnection-wide procedure shall follow the curtailments as directed by the Interconnection-wide procedure. A Reliability Coordinator desiring to use a local procedure as a substitute for curtailments as directed by the Interconnection-wide procedure shall obtain prior approval of the local procedure from the ERO. [Time Horizon: Operations Planning]	LOWER
IRO-006-4	R4.	When Interconnection-wide procedures are implemented to curtail Interchange Transactions that cross an Interconnection boundary, each Reliability Coordinator shall comply with the provisions of the Interconnection-wide procedure. [Time Horizon: Real-time Operations]	MEDIUM
IRO-006-4	R5.	During the implementation of relief procedures, and up to the point that emergency action is necessary, Reliability Coordinators and Balancing Authorities shall comply with applicable Interchange scheduling standards. [Time Horizon: Real-time Operations]	MEDIUM
IRO-014-1	R1.	The Reliability Coordinator shall have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability. These Operating Procedures, Processes, or Plans shall address Scenarios that affect other Reliability Coordinator Areas as well as those developed in coordination with other Reliability Coordinators.	MEDIUM
IRO-014-1	R1.1.	These Operating Procedures, Processes, or Plans shall collectively address, as a minimum, the following:	LOWER
IRO-014-1	R1.1.1.	Communications and notifications, including the conditions under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators.	MEDIUM
IRO-014-1	R1.1.2.	Energy and capacity shortages.	MEDIUM
IRO-014-1	R1.1.3.	Planned or unplanned outage information.	MEDIUM
IRO-014-1	R1.1.4.	Voltage control, including the coordination of reactive resources for voltage control.	MEDIUM
IRO-014-1	R1.1.5.	Coordination of information exchange to support reliability assessments.	LOWER
IRO-014-1	R1.1.6.	Authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-014-1	R2.	Each Reliability Coordinator's Operating Procedure, Process, or Plan that requires one or more other Reliability Coordinators to take action (e.g., make notifications, exchange information, or coordinate actions) shall be:	LOWER
IRO-014-1	R2.1.	Agreed to by all the Reliability Coordinators required to take the indicated action(s).	LOWER
IRO-014-1	R2.2.	Distributed to all Reliability Coordinators that are required to take the indicated action(s).	LOWER
IRO-014-1	R3.	A Reliability Coordinator's Operating Procedures, Processes, or Plans developed to support a Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan shall include:	MEDIUM
IRO-014-1	R3.1.	A reference to the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	MEDIUM
IRO-014-1	R3.2.	The agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	LOWER
IRO-014-1	R4.	Each of the Operating Procedures, Processes, and Plans addressed in Reliability Standard IRO-014 Requirement 1 and Requirement 3 shall:	LOWER
IRO-014-1	R4.1.	Include version control number or date	LOWER
IRO-014-1	R4.2.	Include a distribution list.	LOWER
IRO-014-1	R4.3.	Be reviewed, at least once every three years, and updated if needed.	LOWER
IRO-015-1	R1.	The Reliability Coordinator shall follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators.	MEDIUM
IRO-015-1	R1.1.	The Reliability Coordinator shall make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas.	MEDIUM
IRO-015-1	R2.	The Reliability Coordinator shall participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.	LOWER
IRO-015-1	R2.1.	The frequency of these conference calls shall be agreed upon by all involved Reliability Coordinators and shall be at least weekly.	LOWER
IRO-015-1	R3.	The Reliability Coordinator shall provide reliability-related information as requested by other Reliability Coordinators.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
IRO-016-1	R1.	The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.	MEDIUM
IRO-016-1	R1.1.	If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.	MEDIUM
IRO-016-1	R1.2.	If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).	MEDIUM
IRO-016-1	R1.2.1.	If time permits, this re-evaluation shall be done before taking corrective actions.	MEDIUM
IRO-016-1	R1.2.2.	If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.	MEDIUM
IRO-016-1	R1.3.	If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.	MEDIUM
IRO-016-1	R2.	The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.	LOWER
MOD-006-0.1	R1.	R1. Each Transmission Service Provider shall document its procedure on the use of Capacity Benefit Margin (CBM) (scheduling of energy against a CBM reservation). The procedure shall include the following three components:	LOWER
MOD-006-0.1	R1.1.	Require that CBM be used only after the following steps have been taken (as time permits): all non-firm sales have been terminated, Direct-Control Load Management has been implemented, and customer interruptible demands have been interrupted. CBM may be used to reestablish Operating Reserves.	LOWER
MOD-006-0.1	R1.2.	Require that CBM shall only be used if the Load-Serving Entity calling for its use is experiencing a generation deficiency and its Transmission Service Provider is also experiencing Transmission Constraints relative to imports of energy on its transmission system.	LOWER
MOD-006-0.1	R1.3.	Describe the conditions under which CBM may be available as Non-Firm Transmission Service.	LOWER
MOD-006-0.1	R2.	Each Transmission Service Provider shall make its CBM use procedure available on a web site accessible by the Regional Reliability Organizations, NERC, and transmission users.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
MOD-007-0	R1.	Each Transmission Service Provider that uses CBM shall report (to the Regional Reliability Organization, NERC and the transmission users) the use of CBM by the Load-Serving Entities' Loads on its system, except for CBM sales as Non-Firm Transmission Service. (This use of CBM shall be consistent with the Transmission Service Provider's procedure for use of CBM.)	LOWER
MOD-007-0	R2.	The Transmission Service Provider shall post the following three items within 15 calendar days after the use of CBM for an Energy Emergency. This posting shall be on a web site accessible by the Regional Reliability Organizations, NERC, and transmission users.	LOWER
MOD-007-0	R2.1.	Circumstances.	LOWER
MOD-007-0	R2.2.	Duration.	LOWER
MOD-007-0	R2.3.	Amount of CBM used.	LOWER
MOD-010-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R 1.	MEDIUM
MOD-010-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide this steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. If no schedule exists, then these entities shall provide the data on request (30 calendar days).	MEDIUM
MOD-012-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R1) shall provide appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	MEDIUM
MOD-012-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R4) shall provide dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. If no schedule exists, then these entities shall provide data on request (30 calendar days).	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
MOD-016-1.1	R1.	The Planning Authority and Regional Reliability Organization shall have documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses.	LOWER
MOD-016-1.1	R1.1.	The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021. The data submittal requirements shall stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.	LOWER
MOD-016-1.1	R2.	The Regional Reliability Organization shall distribute its documentation required in Requirement 1 and any changes to that documentation, to all Planning Authorities that work within its Region.	LOWER
MOD-016-1.1	R2.1.	The Regional Reliability Organization shall make this distribution within 30 calendar days of approval.	LOWER
MOD-016-1.1	R3.	The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area.	LOWER
MOD-016-1.1	R3.1.	The Planning Authority shall make this distribution within 30 calendar days of approval.	LOWER
MOD-017-0.1	R1.	The Load-Serving Entity, Planning Authority and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R1.	MEDIUM
MOD-017-0.1	R1.1.	Integrated hourly demands in megawatts (MW) for the prior year.	MEDIUM
MOD-017-0.1	R1.2.	Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the prior year.	MEDIUM
MOD-017-0.1	R1.3.	Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years.	MEDIUM
MOD-017-0.1	R1.4.	Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested.	MEDIUM
MOD-018-0	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or dispersed basis) shall:	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
MOD-018-0	R1.1.	Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and	MEDIUM
MOD-018-0	R1.2.	Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load.	LOWER
MOD-018-0	R1.3.	Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1.	LOWER
MOD-018-0	R2.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days).	LOWER
MOD-019-0.1	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-1_R 1.	MEDIUM
MOD-020-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days.	LOWER
MOD-021-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed.	LOWER
MOD-021-0	R2.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R 1.	LOWER
MOD-021-0	R3.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days).	LOWER
NUC-001-1	R1.	The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt	LOW

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
NUC-001-1	R2.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements ¹ that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.	LOW
NUC-001-1	R3.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator.	MEDIUM
NUC-001-1	R4.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall:	MEDIUM
NUC-001-1	R4.1.	Incorporate the NPIRs into their operating analyses of the electric system.	
NUC-001-1	R4.2.	Operate the electric system to meet the NPIRs.	
NUC-001-1	R4.3.	Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.	
NUC-001-1	R5.	The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard.	MEDIUM
NUC-001-1	R6.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs.	MEDIUM
NUC-001-1	R7.	Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	MEDIUM
NUC-001-1	R8.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	MEDIUM
NUC-001-1	R9.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2:	LOW
NUC-001-1	R9.1.	Administrative elements:	
NUC-001-1	R9.1.1.	Definitions of key terms used in the agreement.	
NUC-001-1	R9.1.2.	Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.	
NUC-001-1	R9.1.3.	A requirement to review the agreement(s) at least every three years.	
NUC-001-1	R9.1.4.	A dispute resolution mechanism.	
NUC-001-1	R9.2.	Technical requirements and analysis:	
NUC-001-1	R9.2.1.	Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.	
NUC-001-1	R9.2.2.	Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.	
NUC-001-1	R9.2.3.	Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.	
NUC-001-1	R9.3.	Operations and maintenance coordination:	

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
NUC-001-1	R9.3.1.	Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.	
NUC-001-1	R9.3.2.	Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.	
NUC-001-1	R9.3.3.	Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.	
NUC-001-1	R9.3.4.	Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.	
NUC-001-1	R9.3.5.	Provision to consider nuclear plant coping times required by the NPLRs and their relation to the coordination of grid and nuclear plant restoration following a nuclear plant loss of Off-site Power.	
NUC-001-1	R9.3.6.	Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.	
NUC-001-1	R9.3.7.	Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.	
NUC-001-1	R9.4.	Communications and training:	
NUC-001-1	R9.4.1.	Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.	
NUC-001-1	R9.4.2.	Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.	
NUC-001-1	R9.4.3.	Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.	
NUC-001-1	R9.4.4.	Provisions for supplying information necessary to report to government agencies, as related to NPIRs.	
NUC-001-1	R9.4.5.	Provisions for personnel training, as related to NPIRs.	
PER-001-0	R1.	Each Transmission Operator and Balancing Authority shall provide operating personnel with the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PER-002-0	R1.	Each Transmission Operator and Balancing Authority shall be staffed with adequately trained operating personnel.	HIGH
PER-002-0	R2.	Each Transmission Operator and Balancing Authority shall have a training program for all operating personnel that are in:	HIGH
PER-002-0	R2.1.	Positions that have the primary responsibility, either directly or through communications with others, for the real-time operation of the interconnected Bulk Electric System.	HIGH
PER-002-0	R2.2.	Positions directly responsible for complying with NERC standards.	HIGH
PER-002-0	R3.	For personnel identified in Requirement R2, the Transmission Operator and Balancing Authority shall provide a training program meeting the following criteria:	HIGH
PER-002-0	R3.1.	A set of training program objectives must be defined, based on NERC and Regional Reliability Organization standards, entity operating procedures, and applicable regulatory requirements. These objectives shall reference the knowledge and competencies needed to apply those standards, procedures, and requirements to normal, emergency, and restoration conditions for the Transmission Operator and Balancing Authority operating positions.	MEDIUM
PER-002-0	R3.2.	The training program must include a plan for the initial and continuing training of Transmission Operator and Balancing Authority operating personnel. That plan shall address knowledge and competencies required for reliable system operations.	MEDIUM
PER-002-0	R3.3.	The training program must include training time for all Transmission Operator and Balancing Authority operating personnel to ensure their operating proficiency.	LOWER
PER-002-0	R3.4.	Training staff must be identified, and the staff must be competent in both knowledge of system operations and instructional capabilities.	LOWER
PER-002-0	R4.	For personnel identified in Requirement R2, each Transmission Operator and Balancing Authority shall provide its operating personnel at least five days per year of training and drills using realistic simulations of system emergencies, in addition to other training required to maintain qualified operating personnel.	HIGH
PER-003-0	R1.	Each Transmission Operator, Balancing Authority, and Reliability Coordinator shall staff all operating positions that meet both of the following criteria with personnel that are NERC-certified for the applicable functions:	HIGH
PER-003-0	R1.1.	Positions that have the primary responsibility, either directly or through communications with others, for the real-time operation of the interconnected Bulk Electric System.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PER-003-0	R1.2.	Positions directly responsible for complying with NERC standards.	HIGH
PER-004-1	R1.	Each Reliability Coordinator shall be staffed with adequately trained and NERC-certified Reliability Coordinator operators, 24 hours per day, seven days per week.	HIGH
PER-004-1	R2.	All Reliability Coordinator operating personnel shall each complete a minimum of five days per year of training and drills using realistic simulations of system emergencies, in addition to other training required to maintain qualified operating personnel.	HIGH
PER-004-1	R3.	Reliability Coordinator operating personnel shall have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	HIGH
PER-004-1	R4.	Reliability Coordinator operating personnel shall have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.	HIGH
PER-004-1	R5.	Reliability Coordinator operating personnel shall place particular attention on SOLs and IROLs and inter-tie facility limits. The Reliability Coordinator shall ensure protocols are in place to allow Reliability Coordinator operating personnel to have the best available information at all times.	HIGH
PRC-001-1	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.	HIGH
PRC-001-1	R2.	Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:	HIGH
PRC-001-1	R2.1.	If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.	HIGH
PRC-001-1	R2.2.	If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.	HIGH
PRC-001-1	R3.	A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.	<blank>
PRC-001-1	R3.1.	Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PRC-001-1	R3.2.	Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.	HIGH
PRC-001-1	R4.	Each Transmission Operator shall coordinate protection systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.	HIGH
PRC-001-1	R5.	A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the protection systems of others:	HIGH
PRC-001-1	R5.1.	Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.	HIGH
PRC-001-1	R5.2.	Each Transmission Operator shall notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems.	HIGH
PRC-001-1	R6.	Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.	HIGH
PRC-004-1	R1.	The Transmission Owner and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Reliability Organization's procedures developed for Reliability Standard PRC-003 Requirement 1.	HIGH
PRC-004-1	R2.	The Generator Owner shall analyze its generator Protection System Misoperations, and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	HIGH
PRC-004-1	R3.	The Transmission Owner, any Distribution Provider that owns a transmission Protection System, and the Generator Owner shall each provide to its Regional Reliability Organization, documentation of its Misoperations analyses and Corrective Action Plans according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	LOWER
PRC-005-1	R1.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:	HIGH
PRC-005-1	R1.1.	Maintenance and testing intervals and their basis.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PRC-005-1	R1.2.	Summary of maintenance and testing procedures.	HIGH
PRC-005-1	R2.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include:	LOWER
PRC-005-1	R2.1.	Evidence Protection System devices were maintained and tested within the defined intervals.	HIGH
PRC-005-1	R2.2.	Date each Protection System device was last tested/maintained.	HIGH
PRC-007-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall ensure that its UFLS program is consistent with its Regional Reliability Organization's UFLS program requirements.	MEDIUM
PRC-007-0	R2.	The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database.	LOWER
PRC-007-0	R3.	The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days).	LOWER
PRC-008-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.	MEDIUM
PRC-008-0	R2.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).	MEDIUM
PRC-009-0	R1.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PRC-009-0	R1.1.	A description of the event including initiating conditions.	MEDIUM
PRC-009-0	R1.2.	A review of the UFLS set points and tripping times.	MEDIUM
PRC-009-0	R1.3.	A simulation of the event.	MEDIUM
PRC-009-0	R1.4.	A summary of the findings.	MEDIUM
PRC-009-0	R2.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.	LOWER
PRC-010-0	R1.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).	MEDIUM
PRC-010-0	R1.1.	This assessment shall include, but is not limited to:	MEDIUM
PRC-010-0	R1.1.1.	Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.	MEDIUM
PRC-010-0	R1.1.2.	Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.	MEDIUM
PRC-010-0	R1.1.3.	A review of the voltage set points and timing.	MEDIUM
PRC-010-0	R2.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).	LOWER
PRC-011-0	R1.	The Transmission Owner and Distribution Provider that owns a UVLS system shall have a UVLS equipment maintenance and testing program in place. This program shall include:	MEDIUM
PRC-011-0	R1.1.	The UVLS system identification which shall include but is not limited to:	MEDIUM
PRC-011-0	R1.1.1.	Relays.	MEDIUM
PRC-011-0	R1.1.2.	Instrument transformers.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PRC-011-0	R1.1.3.	Communications systems, where appropriate.	MEDIUM
PRC-011-0	R1.1.4.	Batteries.	MEDIUM
PRC-011-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	MEDIUM
PRC-011-0	R1.3.	Summary of testing procedure.	MEDIUM
PRC-011-0	R1.4.	Schedule for system testing.	MEDIUM
PRC-011-0	R1.5.	Schedule for system maintenance.	MEDIUM
PRC-011-0	R1.6.	Date last tested/maintained.	MEDIUM
PRC-011-0	R2.	The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days).	LOWER
PRC-015-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall maintain a list of and provide data for existing and proposed SPSs as specified in Reliability Standard PRC-013-0_R 1.	MEDIUM
PRC-015-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have evidence it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures as defined in Reliability Standard PRC-012-0_R1 prior to being placed in service.	MEDIUM
PRC-015-0	R3.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days).	LOWER
PRC-016-0.1	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall analyze its SPS operations and maintain a record of all misoperations in accordance with the Regional SPS review procedure specified in Reliability Standard PRC-012-0_R1.	MEDIUM
PRC-016-0.1	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall take corrective actions to avoid future misoperations.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PRC-016-0.1	R3.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days).	LOWER
PRC-017-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have a system maintenance and testing program(s) in place. The program(s) shall include:	HIGH
PRC-017-0	R1.1.	SPS identification shall include but is not limited to:	HIGH
PRC-017-0	R1.1.1.	Relays.	HIGH
PRC-017-0	R1.1.2.	Instrument transformers.	HIGH
PRC-017-0	R1.1.3.	Communications systems, where appropriate.	HIGH
PRC-017-0	R1.1.4.	Batteries.	HIGH
PRC-017-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	HIGH
PRC-017-0	R1.3.	Summary of testing procedure.	HIGH
PRC-017-0	R1.4.	Schedule for system testing.	HIGH
PRC-017-0	R1.5.	Schedule for system maintenance.	HIGH
PRC-017-0	R1.6.	Date last tested/maintained.	MEDIUM
PRC-017-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days).	LOWER
PRC-018-1	R1.	Each Transmission Owner and Generator Owner required to install DMEs by its Regional Reliability Organization (reliability standard PRC-002 Requirements 1-3) shall have DMEs installed that meet the following requirements:	LOWER
PRC-018-1	R1.1.	Internal Clocks in DME devices shall be synchronized to within 2 milliseconds or less of Universal Coordinated Time scale (UTC)	LOWER
PRC-018-1	R1.2.	Recorded data from each Disturbance shall be retrievable for ten calendar days..	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PRC-018-1	R2.	The Transmission Owner and Generator Owner shall each install DMEs in accordance with its Regional Reliability Organization's installation requirements (reliability standard PRC-002 Requirements 1 through 3).	LOWER
PRC-018-1	R3.	The Transmission Owner and Generator Owner shall each maintain, and report to its Regional Reliability Organization on request, the following data on the DMEs installed to meet that region's installation requirements (reliability standard PRC-002 Requirements 1.1, 2.1 and 3.1):	LOWER
PRC-018-1	R3.1.	Type of DME (sequence of event recorder, fault recorder, or dynamic disturbance recorder).	LOWER
PRC-018-1	R3.2.	Make and model of equipment.	LOWER
PRC-018-1	R3.3.	Installation location.	LOWER
PRC-018-1	R3.4.	Operational status.	LOWER
PRC-018-1	R3.5.	Date last tested.	LOWER
PRC-018-1	R3.6.	Monitored elements, such as transmission circuit, bus section, etc.	LOWER
PRC-018-1	R3.7.	Monitored devices, such as circuit breaker, disconnect status, alarms, etc.	LOWER
PRC-018-1	R3.8.	Monitored electrical quantities, such as voltage, current, etc.	LOWER
PRC-018-1	R4.	The Transmission Owner and Generator Owner shall each provide Disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements (reliability standard PRC-002 Requirement 4).	LOWER
PRC-018-1	R5.	The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years.	LOWER
PRC-018-1	R6.	Each Transmission Owner and Generator Owner that is required by its Regional Reliability Organization to have DMEs shall have a maintenance and testing program for those DMEs that includes:	LOWER
PRC-018-1	R6.1.	Maintenance and testing intervals and their basis.	LOWER
PRC-018-1	R6.2.	Summary of maintenance and testing procedures.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
PRC-021-1	R1.	Each Transmission Owner and Distribution Provider that owns a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall annually update its UVLS data to support the Regional UVLS program database. The following data shall be provided to the Regional Reliability Organization for each installed UVLS system:	LOWER
PRC-021-1	R1.1.	Size and location of customer load, or percent of connected load, to be interrupted.	LOWER
PRC-021-1	R1.2.	Corresponding voltage set points and overall scheme clearing times.	MEDIUM
PRC-021-1	R1.3.	Time delay from initiation to trip signal.	LOWER
PRC-021-1	R1.4.	Breaker operating times.	LOWER
PRC-021-1	R1.5.	Any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	LOWER
PRC-021-1	R2.	Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request.	LOWER
PRC-022-1	R1.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:	MEDIUM
PRC-022-1	R1.1.	A description of the event including initiating conditions.	LOWER
PRC-022-1	R1.2.	A review of the UVLS set points and tripping times.	MEDIUM
PRC-022-1	R1.3.	A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.	LOWER
PRC-022-1	R1.4.	A summary of the findings.	LOWER
PRC-022-1	R1.5.	For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.	MEDIUM
PRC-022-1	R2.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.	LOWER
TOP-001-1	R1.	Each Transmission Operator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its area and shall exercise specific authority to alleviate operating emergencies.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TOP-001-1	R2.	Each Transmission Operator shall take immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.	HIGH
TOP-001-1	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.	HIGH
TOP-001-1	R4.	Each Distribution Provider and Load-Serving Entity shall comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions.	HIGH
TOP-001-1	R5.	Each Transmission Operator shall inform its Reliability Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, and take actions to avoid, when possible, or mitigate the emergency.	HIGH
TOP-001-1	R6.	Each Transmission Operator, Balancing Authority, and Generator Operator shall render all available emergency assistance to others as requested, provided that the requesting entity has implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements.	HIGH
TOP-001-1	R7.	Each Transmission Operator and Generator Operator shall not remove Bulk Electric System facilities from service if removing those facilities would burden neighboring systems unless:	HIGH
TOP-001-1	R7.1.	For a generator outage, the Generator Operator shall notify and coordinate with the Transmission Operator. The Transmission Operator shall notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	HIGH
TOP-001-1	R7.2.	For a transmission facility, the Transmission Operator shall notify and coordinate with its Reliability Coordinator. The Transmission Operator shall notify other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TOP-001-1	R7.3.	When time does not permit such notifications and coordination, or when immediate action is required to prevent a hazard to the public, lengthy customer service interruption, or damage to facilities, the Generator Operator shall notify the Transmission Operator, and the Transmission Operator shall notify its Reliability Coordinator and adjacent Transmission Operators, at the earliest possible time.	HIGH
TOP-001-1	R8.	During a system emergency, the Balancing Authority and Transmission Operator shall immediately take action to restore the Real and Reactive Power Balance. If the Balancing Authority or Transmission Operator is unable to restore Real and Reactive Power Balance it shall request emergency assistance from the Reliability Coordinator. If corrective action or emergency assistance is not adequate to mitigate the Real and Reactive Power Balance, then the Reliability Coordinator, Balancing Authority, and Transmission Operator shall implement firm load shedding.	HIGH
TOP-002-2	R1.	Each Balancing Authority and Transmission Operator shall maintain a set of current plans that are designed to evaluate options and set procedures for reliable operation through a reasonable future time period. In addition, each Balancing Authority and Transmission Operator shall be responsible for using available personnel and system equipment to implement these plans to ensure that interconnected system reliability will be maintained.	MEDIUM
TOP-002-2	R2.	Each Balancing Authority and Transmission Operator shall ensure its operating personnel participate in the system planning and design study processes, so that these studies contain the operating personnel perspective and system operating personnel are aware of the planning purpose.	MEDIUM
TOP-002-2	R3.	Each Load-Serving Entity and Generator Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider. Each Balancing Authority and Transmission Service Provider shall coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.	MEDIUM
TOP-002-2	R4.	Each Balancing Authority and Transmission Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator, so that normal Interconnection operation will proceed in an orderly and consistent manner.	MEDIUM
TOP-002-2	R5.	Each Balancing Authority and Transmission Operator shall plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.	MEDIUM
TOP-002-2	R6.	Each Balancing Authority and Transmission Operator shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional, and local reliability requirements.	MEDIUM
TOP-002-2	R7.	Each Balancing Authority shall plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TOP-002-2	R8.	Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.	MEDIUM
TOP-002-2	R9.	Each Balancing Authority shall plan to meet Interchange Schedules and Ramps.	LOWER
TOP-002-2	R10.	Each Balancing Authority and Transmission Operator shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).	MEDIUM
TOP-002-2	R11.	The Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs. Neighboring Transmission Operators shall utilize identical SOLs for common facilities. The Transmission Operator shall update these Bulk Electric System studies as necessary to reflect current system conditions; and shall make the results of Bulk Electric System studies available to the Transmission Operators, Balancing Authorities (subject to confidentiality requirements), and to its Reliability Coordinator.	MEDIUM
TOP-002-2	R12.	The Transmission Service Provider shall include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available Transfer Capability calculation processes.	MEDIUM
TOP-002-2	R13.	At the request of the Balancing Authority or Transmission Operator, a Generator Operator shall perform generating real and reactive capability verification that shall include, among other variables, weather, ambient air and water conditions, and fuel quality and quantity, and provide the results to the Balancing Authority or Transmission Operator operating personnel as requested.	MEDIUM
TOP-002-2	R14.	Generator Operators shall, without any intentional time delay, notify their Balancing Authority and Transmission Operator of changes in capabilities and characteristics including but not limited to:	MEDIUM
TOP-002-2	R14.1.	Changes in real output capabilities.	MEDIUM
TOP-002-2	R14.2.	Automatic Voltage Regulator status and mode setting. (Retired August 1, 2007)	LOWER
TOP-002-2	R15.	Generation Operators shall, at the request of the Balancing Authority or Transmission Operator, provide a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).	LOWER
TOP-002-2	R16.	Subject to standards of conduct and confidentiality agreements, Transmission Operators shall, without any intentional time delay, notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics including but not limited to:	MEDIUM
TOP-002-2	R16.1.	Changes in transmission facility status.	HIGH
TOP-002-2	R16.2.	Changes in transmission facility rating.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TOP-002-2	R17.	Balancing Authorities and Transmission Operators shall, without any intentional time delay, communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.	HIGH
TOP-002-2	R18.	Neighboring Balancing Authorities, Transmission Operators, Generator Operators, Transmission Service Providers, and Load-Serving Entities shall use uniform line identifiers when referring to transmission facilities of an interconnected network.	MEDIUM
TOP-002-2	R19.	Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations.	MEDIUM
TOP-003-0	R1.	Generator Operators and Transmission Operators shall provide planned outage information.	<blank>
TOP-003-0	R1.1.	Each Generator Operator shall provide outage information daily to its Transmission Operator for scheduled generator outages planned for the next day (any foreseen outage of a generator greater than 50 MW). The Transmission Operator shall establish the outage reporting requirements.	MEDIUM
TOP-003-0	R1.2.	Each Transmission Operator shall provide outage information daily to its Reliability Coordinator, and to affected Balancing Authorities and Transmission Operators for scheduled generator and bulk transmission outages planned for the next day (any foreseen outage of a transmission line or transformer greater than 100 kV or generator greater than 50 MW) that may collectively cause or contribute to an SOL or IROL violation or a regional operating area limitation. The Reliability Coordinator shall establish the outage reporting requirements.	MEDIUM
TOP-003-0	R1.3.	Such information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.	MEDIUM
TOP-003-0	R2.	Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of system voltage regulating equipment, such as automatic voltage regulators on generators, supplementary excitation control, synchronous condensers, shunt and series capacitors, reactors, etc., among affected Balancing Authorities and Transmission Operators as required.	MEDIUM
TOP-003-0	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of telemetering and control equipment and associated communication channels between the affected areas.	MEDIUM
TOP-003-0	R4.	Each Reliability Coordinator shall resolve any scheduling of potential reliability conflicts.	MEDIUM
TOP-004-2	R1.	Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).	

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TOP-004-2	R2.	Each Transmission Operator shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.	
TOP-004-2	R3.	Each Transmission Operator shall operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by its Reliability Coordinator.	
TOP-004-2	R4.	If a Transmission Operator enters an unknown operating state (i.e. any state for which valid operating limits have not been determined), it will be considered to be in an emergency and shall restore operations to respect proven reliable power system limits within 30 minutes.	
TOP-004-2	R5.	Each Transmission Operator shall make every effort to remain connected to the Interconnection. If the Transmission Operator determines that by remaining interconnected, it is in imminent danger of violating an IROL or SOL, the Transmission Operator may take such actions, as it deems necessary, to protect its area.	
TOP-004-2	R6.	Transmission Operators, individually and jointly with other Transmission Operators, shall develop, maintain, and implement formal policies and procedures to provide for transmission reliability. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including:	
TOP-004-2	R6.1.	Monitoring and controlling voltage levels and real and reactive power flows.	
TOP-004-2	R6.2.	Switching transmission elements.	
TOP-004-2	R6.3.	Planned outages of transmission elements.	
TOP-004-2	R6.4.	Responding to IROL and SOL violations.	
TOP-005-1.1	R1.	Each Transmission Operator and Balancing Authority shall provide its Reliability Coordinator with the operating data that the Reliability Coordinator requires to perform operational reliability assessments and to coordinate reliable operations within the Reliability Coordinator Area.	MEDIUM
TOP-005-1.1	R1.1.	Each Reliability Coordinator shall identify the data requirements from the list in Attachment 1-TOP-005-0 "Electric System Reliability Data" and any additional operating information requirements relating to operation of the bulk power system within the Reliability Coordinator Area.	MEDIUM
TOP-005-1.1	R2.	As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TOP-005-1.1	R3.	Upon request, each Balancing Authority and Transmission Operator shall provide to other Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability, the operating data that are necessary to allow these Balancing Authorities and Transmission Operators to perform operational reliability assessments and to coordinate reliable operations. Balancing Authorities and Transmission Operators shall provide the types of data as listed in Attachment 1-TOP-005-0 "Electric System Reliability Data," unless otherwise agreed to by the Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability.	MEDIUM
TOP-005-1.1	R4.	Each Purchasing-Selling Entity shall provide information as requested by its Host Balancing Authorities and Transmission Operators to enable them to conduct operational reliability assessments and coordinate reliable operations.	MEDIUM
TOP-006-1	R1.	Each Transmission Operator and Balancing Authority shall know the status of all generation and transmission resources available for use.	MEDIUM
TOP-006-1	R1.1.	Each Generator Operator shall inform its Host Balancing Authority and the Transmission Operator of all generation resources available for use.	MEDIUM
TOP-006-1	R1.2.	Each Transmission Operator and Balancing Authority shall inform the Reliability Coordinator and other affected Balancing Authorities and Transmission Operators of all generation and transmission resources available for use.	MEDIUM
TOP-006-1	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources.	HIGH
TOP-006-1	R3.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide appropriate technical information concerning protective relays to their operating personnel.	MEDIUM
TOP-006-1	R4.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have information, including weather forecasts and past load patterns, available to predict the system's near-term load pattern.	MEDIUM
TOP-006-1	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions and to indicate, if appropriate, the need for corrective action.	MEDIUM
TOP-006-1	R6.	Each Balancing Authority and Transmission Operator shall use sufficient metering of suitable range, accuracy and sampling rate (if applicable) to ensure accurate and timely monitoring of operating conditions under both normal and emergency situations.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TOP-006-1	R7.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor system frequency.	HIGH
TOP-007-0	R1.	A Transmission Operator shall inform its Reliability Coordinator when an IROL or SOL has been exceeded and the actions being taken to return the system to within limits.	HIGH
TOP-007-0	R2.	Following a Contingency or other event that results in an IROL violation, the Transmission Operator shall return its transmission system to within IROL as soon as possible, but not longer than 30 minutes.	HIGH
TOP-007-0	R3.	A Transmission Operator shall take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to comply with Requirement R 2.	HIGH
TOP-007-0	R4.	The Reliability Coordinator shall evaluate actions taken to address an IROL or SOL violation and, if the actions taken are not appropriate or sufficient, direct actions required to return the system to within limits.	HIGH
TOP-008-1	R1.	The Transmission Operator experiencing or contributing to an IROL or SOL violation shall take immediate steps to relieve the condition, which may include shedding firm load.	HIGH
TOP-008-1	R2.	Each Transmission Operator shall operate to prevent the likelihood that a disturbance, action, or inaction will result in an IROL or SOL violation in its area or another area of the Interconnection. In instances where there is a difference in derived operating limits, the Transmission Operator shall always operate the Bulk Electric System to the most limiting parameter.	HIGH
TOP-008-1	R3.	The Transmission Operator shall disconnect the affected facility if the overload on a transmission facility or abnormal voltage or reactive condition persists and equipment is endangered. In doing so, the Transmission Operator shall notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection prior to switching, if time permits, otherwise, immediately thereafter.	HIGH
TOP-008-1	R4.	The Transmission Operator shall have sufficient information and analysis tools to determine the cause(s) of SOL violations. This analysis shall be conducted in all operating timeframes. The Transmission Operator shall use the results of these analyses to immediately mitigate the SOL violation.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TPL-001-0.1	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that, with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services at all Demand levels over the range of forecast system demands, under the conditions defined in Category A of Table I. To be considered valid, the Planning Authority and Transmission Planner assessments shall:	HIGH
TPL-001-0.1	R1.1.	Be made annually.	MEDIUM
TPL-001-0.1	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	MEDIUM
TPL-001-0.1	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category A of Table 1 (no contingencies). The specific elements selected (from each of the following categories) shall be acceptable to the associated Regional Reliability Organization(s).	MEDIUM
TPL-001-0.1	R1.3.1.	Cover critical system conditions and study years as deemed appropriate by the entity performing the study.	MEDIUM
TPL-001-0.1	R1.3.2.	Be conducted annually unless changes to system conditions do not warrant such analyses.	MEDIUM
TPL-001-0.1	R1.3.3.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	MEDIUM
TPL-001-0.1	R1.3.4.	Have established normal (pre-contingency) operating procedures in place.	MEDIUM
TPL-001-0.1	R1.3.5.	Have all projected firm transfers modeled.	MEDIUM
TPL-001-0.1	R1.3.6.	Be performed for selected demand levels over the range of forecast system demands.	MEDIUM
TPL-001-0.1	R1.3.7.	Demonstrate that system performance meets Table 1 for Category A (no contingencies).	MEDIUM
TPL-001-0.1	R1.3.8.	Include existing and planned facilities.	MEDIUM
TPL-001-0.1	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	MEDIUM
TPL-001-0.1	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category A.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TPL-001-0.1	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-001-0_R1, the Planning Authority and Transmission Planner shall each:	MEDIUM
TPL-001-0.1	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon.	MEDIUM
TPL-001-0.1	R2.1.1.	Including a schedule for implementation.	MEDIUM
TPL-001-0.1	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	MEDIUM
TPL-001-0.1	R2.1.3.	Consider lead times necessary to implement plans.	MEDIUM
TPL-001-0.1	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	LOWER
TPL-001-0.1	R3.	The Planning Authority and Transmission Planner shall each document the results of these reliability assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	LOWER
TPL-002-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I. To be valid, the Planning Authority and Transmission Planner assessments shall:	HIGH
TPL-002-0	R1.1.	Be made annually.	MEDIUM
TPL-002-0	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	MEDIUM
TPL-002-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category B of Table 1 (single contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	MEDIUM
TPL-002-0	R1.3.1.	Be performed and evaluated only for those Category B contingencies that would produce the more severe System results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TPL-002-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	MEDIUM
TPL-002-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	MEDIUM
TPL-002-0	R1.3.4.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	MEDIUM
TPL-002-0	R1.3.5.	Have all projected firm transfers modeled.	MEDIUM
TPL-002-0	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast system Demands.	MEDIUM
TPL-002-0	R1.3.7.	Demonstrate that system performance meets Category B contingencies.	MEDIUM
TPL-002-0	R1.3.8.	Include existing and planned facilities.	MEDIUM
TPL-002-0	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	MEDIUM
TPL-002-0	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	MEDIUM
TPL-002-0	R1.3.11.	Include the effects of existing and planned control devices.	MEDIUM
TPL-002-0	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.	MEDIUM
TPL-002-0	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category B of Table I.	MEDIUM
TPL-002-0	R1.5.	Consider all contingencies applicable to Category B.	MEDIUM
TPL-002-0	R2.	When System simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-002-0_R1, the Planning Authority and Transmission Planner shall each:	MEDIUM
TPL-002-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	MEDIUM
TPL-002-0	R2.1.1.	Including a schedule for implementation.	MEDIUM
TPL-002-0	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TPL-002-0	R2.1.3.	Consider lead times necessary to implement plans.	MEDIUM
TPL-002-0	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	MEDIUM
TPL-002-0	R3.	The Planning Authority and Transmission Planner shall each document the results of its Reliability Assessments and corrective plans and shall annually provide the results to its respective Regional Reliability Organization(s), as required by the Regional Reliability Organization.	LOWER
TPL-003-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard. To be valid, the Planning Authority and Transmission Planner assessments shall:	HIGH
TPL-003-0	R1.1.	Be made annually.	MEDIUM
TPL-003-0	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	MEDIUM
TPL-003-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category C of Table 1 (multiple contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	MEDIUM
TPL-003-0	R1.3.1.	Be performed and evaluated only for those Category C contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.	MEDIUM
TPL-003-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	MEDIUM
TPL-003-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	MEDIUM
TPL-003-0	R1.3.4.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	MEDIUM
TPL-003-0	R1.3.5.	Have all projected firm transfers modeled.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TPL-003-0	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast system demands.	MEDIUM
TPL-003-0	R1.3.7.	Demonstrate that System performance meets Table 1 for Category C contingencies.	MEDIUM
TPL-003-0	R1.3.8.	Include existing and planned facilities.	MEDIUM
TPL-003-0	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet System performance.	MEDIUM
TPL-003-0	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	MEDIUM
TPL-003-0	R1.3.11.	Include the effects of existing and planned control devices.	MEDIUM
TPL-003-0	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those Demand levels for which planned (including maintenance) outages are performed.	MEDIUM
TPL-003-0	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category C.	MEDIUM
TPL-003-0	R1.5.	Consider all contingencies applicable to Category C.	MEDIUM
TPL-003-0	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-003-0_R1, the Planning Authority and Transmission Planner shall each:	MEDIUM
TPL-003-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	MEDIUM
TPL-003-0	R2.1.1.	Including a schedule for implementation.	MEDIUM
TPL-003-0	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	MEDIUM
TPL-003-0	R2.1.3.	Consider lead times necessary to implement plans.	MEDIUM
TPL-003-0	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	MEDIUM
TPL-003-0	R3.	The Planning Authority and Transmission Planner shall each document the results of these Reliability Assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	LOWER

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TPL-004-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is evaluated for the risks and consequences of a number of each of the extreme contingencies that are listed under Category D of Table I. To be valid, the Planning Authority's and Transmission Planner's assessment shall:	MEDIUM
TPL-004-0	R1.1.	Be made annually.	MEDIUM
TPL-004-0	R1.2.	Be conducted for near-term (years one through five).	MEDIUM
TPL-004-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category D contingencies of Table I. The specific elements selected (from within each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	MEDIUM
TPL-004-0	R1.3.1.	Be performed and evaluated only for those Category D contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.	MEDIUM
TPL-004-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	MEDIUM
TPL-004-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	MEDIUM
TPL-004-0	R1.3.4.	Have all projected firm transfers modeled.	MEDIUM
TPL-004-0	R1.3.5.	Include existing and planned facilities.	MEDIUM
TPL-004-0	R1.3.6.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	MEDIUM
TPL-004-0	R1.3.7.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	MEDIUM
TPL-004-0	R1.3.8.	Include the effects of existing and planned control devices.	MEDIUM
TPL-004-0	R1.3.9.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.	MEDIUM
TPL-004-0	R1.4.	Consider all contingencies applicable to Category D.	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
TPL-004-0	R2.	The Planning Authority and Transmission Planner shall each document the results of its reliability assessments and shall annually provide the results to its entities' respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	LOWER
VAR-001-1	R1.	Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.	HIGH
VAR-001-1	R2.	Each Transmission Operator shall acquire sufficient reactive resources within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	HIGH
VAR-001-1	R3.	The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.	LOWER
VAR-001-1	R3.1.	Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.	LOWER
VAR-001-1	R3.2.	For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.	LOWER
VAR-001-1	R4.	Each Transmission Operator shall specify a voltage or Rreactive Power schedule at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).	MEDIUM
VAR-001-1	R5.	Each Purchasing-Selling Entity shall arrange for (self-provide or purchase) reactive resources to satisfy its reactive requirements identified by its Transmission Service Provider.	HIGH
VAR-001-1	R6.	The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.	MEDIUM
VAR-001-1	R6.1.	When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.	MEDIUM
VAR-001-1	R7.	The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.	HIGH

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
VAR-001-1	R8.	Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – including reactive generation scheduling; transmission line and reactive resource switching; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.	HIGH
VAR-001-1	R9.	Each Transmission Operator shall maintain reactive resources to support its voltage under first Contingency conditions.	HIGH
VAR-001-1	R9.1.	Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.	HIGH
VAR-001-1	R10.	Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.	HIGH
VAR-001-1	R11.	After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.	LOWER
VAR-001-1	R12.	The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.	HIGH
VAR-002-1.1a	R1.	The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator.	MEDIUM
VAR-002-1.1a	R2.	Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings. [1] as directed by the Transmission Operator	MEDIUM
VAR-002-1.1a	R2.1.	When a generator's automatic voltage regulator is out of service, the Generator Operator shall use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.	MEDIUM
VAR-002-1.1a	R2.2.	When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.	MEDIUM
VAR-002-1.1a	R3.	Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:	MEDIUM

FERC Approved Standards

Standard Number	Requirement Number	Text of Requirement	Violation Risk Factors
VAR-002-1.1a	R3.1.	A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.	MEDIUM
VAR-002-1.1a	R3.2.	A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.	MEDIUM
VAR-002-1.1a	R4.	The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.	LOWER
VAR-002-1.1a	R4.1.	For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:	LOWER
VAR-002-1.1a	R4.1.1.	Tap settings.	LOWER
VAR-002-1.1a	R4.1.2.	Available fixed tap ranges.	LOWER
VAR-002-1.1a	R4.1.3.	Impedance data.	LOWER
VAR-002-1.1a	R4.1.4.	The +/- voltage range with step-change in % for load-tap changing transformers.	LOWER
VAR-002-1.1a	R5.	After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.	MEDIUM
VAR-002-1.1a	R5.1.	If the Generator Operator can't comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.	LOWER