

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

Index:

Standard Number CIP-002-1 Critical Cyber Asset Identification	2
Standard Number CIP-003-1 Security Management Controls	54
Standard Number CIP-004-1 Personnel & Training.....	119
Standard Number CIP-005-1 Electronic Security Perimeter(s).....	1613
Standard Number CIP-006-1 Physical Security of Critical Cyber Assets.....	2421
Standard Number CIP-007-1 Systems Security Management.....	3026
Standard Number CIP-008-1 Incident Reporting and Response Planning.....	4035
Standard Number CIP-009-1 Recovery Plans for Critical Cyber Assets	4136

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 <u>which includes evaluation criteria, but does not include procedures, but includes evaluation criteria.</u>	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but <u>does not include</u> 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	<u>The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.</u> The Responsible Entity has developed a list of Critical Cyber Assets but the list has not been reviewed and	The Responsible Entity did not develop a list of <u>associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2</u> its identified Critical Cyber Assets even if such list is null.

Standard Number CIP-002-1 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
			updated annually as required.	
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 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.

Standard Number CIP-002-1 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	N/A	N/A	<p>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.</p> <p><u>OR</u></p> <p><u>The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of of the list of Critical Cyber Assets (even if such lists are null.)</u></p>	<p>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.)</p>

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	The senior manager is identified by name, title, and date of designation but the designation is	The senior manager is identified by business phone and business address but the designation is	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
		<u>missing business phone or business address</u> N/A	<u>missing one of the following: name, title, or date of designation</u> N/A	of designation.
R2.2.	<u>Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.</u> N/A	<u>Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.</u> N/A	<u>Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.</u> N/A	<u>Changes to the senior manager were documented in 120 or more days of the effective date.</u> 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	<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> <ul style="list-style-type: none"> 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk. 	<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> <ul style="list-style-type: none"> 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	<p>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.</p>	<p>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.</p>
R4.	N/A	<p>The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.</p>	<p><u>The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.</u> The Responsible Entity did not implement but documented a program to identify, classify, and protect information associated with Critical Cyber Assets.</p>	<p>The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.</p>

Standard Number CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.
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.	<u>The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.</u> 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.

Standard Number CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both. 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.
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

Standard Number CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				protected information.
R6.	<p><u>The Responsible Entity has established but not documented a change control process</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity has established but not documented a configuration management process.</u>The Responsible Entity has established but not documented either a change control or configuration management process.</p>	<p><u>The Responsible Entity has established but not documented both a change control process and configuration management process.</u>The Responsible Entity has established but not documented a change control and configuration management process.</p>	<p><u>The Responsible Entity has not established and documented a change control process</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity has not established and documented a configuration management process.</u>The Responsible Entity has not established nor documented either a change control or configuration management process.</p>	<p><u>The Responsible Entity has not established and documented a change control process</u></p> <p><u>AND</u></p> <p><u>The Responsible Entity has not established and documented a configuration management process.</u>The Responsible Entity has not established nor documented a change control and configuration management process.</p>

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.	<p><u>The Responsible Entity established 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.</u></p> <p><u>AND</u></p> <p><u>The Responsible Entity did not provide security awareness reinforcement on at least a quarterly basis.</u>The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.</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 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.	<p><u>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</u></p> <p><u>AND</u></p>	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.

Standard Number CIP-004-1 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<u>The Responsible Entity did not review the training program on an annual basis.</u> The Responsible Entity did not review the training program on an annual basis.		
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	<u>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.</u> N/A	The training does not include one <u>two</u> 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 <u>three</u> or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
R2.3.	N/A	N/A	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.

Standard Number CIP-004-1 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.	<u>The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in more than thirty (30) days of such personnel being granted such access.</u> 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.
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.

Standard Number CIP-004-1 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
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 personnel.	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 such access to Critical Cyber Assets, nor any change in the access rights of such personnel.

Standard Number CIP-004-1 Personnel & Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
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).	<u>The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).</u> The Responsible Entity did not identify and document all Electronic Security Perimeter(s).	<u>The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter.</u> OR <u>The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).</u> 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 Assets 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).

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.
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,	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,	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,	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 Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
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 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	<u>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.</u> The Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party.

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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
R2.6.	The Responsible Entity did not maintain a document identifying the content of the banner. OR 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.	<u>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.</u> 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.	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.	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.
R3.	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not	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.	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.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	implement electronic or manual processes monitoring and logging at less than 5% of the access points.			
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 for monitoring and logging at less than 5% of the access points to dial-up devices.</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.	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.	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.
R3.2.	N/A	N/A	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>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</p>

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	The Responsible Entity did not performed at least annually a Vulnerability Assessment <u>at least annually</u> for more <u>less</u> than <u>95%</u> but less than 100% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not performed at least annually a Vulnerability Assessment <u>at least annually</u> for <u>5% or more</u> than 90% <u>but less than</u> or equal to 95% <u>10%</u> of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not performed at least annually a Vulnerability Assessment <u>at least annually</u> for <u>10% or more</u> than 85% <u>but less than</u> or equal to 90% <u>15%</u> of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not performed at least annually a Vulnerability Assessment <u>at least annually</u> for 85% or less <u>15% or more</u> 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.

Standard Number CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
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 calendar days of the change.	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 controls within ninety calendar days of the change.	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 controls within ninety calendar days of the change.	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 calendar days of the change.
R5.3.	<u>The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.</u> The Responsible Entity did not retain electronic access logs for at least 90 calendar days. N/A	<u>The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.</u> The Responsible Entity retained electronic access logs for more than 90 but less than 120 calendar days. N/A	<u>The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.</u> The responsible Entity retained electronic access logs for 120 calendar days or more but less than 150 calendar days. N/A	<u>The Responsible Entity retained electronic access logs for less than 45 calendar days.</u> 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	<u>The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.</u> The Responsible Entity did not retain electronic access logs for at least 90 calendar days.N/A	<u>The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.</u> The Responsible Entity retained electronic access logs for more than 90 but less than 120 calendar days.N/A	<u>The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.</u> N/AThe Responsible Entity did not retain electronic access logs for 120 calendar days or more but less than 150 calendar days.at least calendar days.	<u>The Responsible Entity retained physical access logs for less than 45 calendar days.</u> 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	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	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	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-006-1 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	R6.3.	R6.3.	R6.3.	

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><u>The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.</u></p> <p><u>AND</u></p> <p><u>The Responsible Entity did not document that testing was performed as required in R1.2</u></p> <p><u>AND</u></p> <p><u>The Responsible Entity did not document the test results as required in R1.3.</u>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>

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.1.	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).	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).	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).	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).
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).
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,	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	The Responsible Entity did not document 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	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

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	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 of the patches and upgrades.	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 patches and upgrades.	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 patches and upgrades.	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 upgrades.
R3.2.	N/A	N/A	N/A	<p><u>The Responsible Entity did not document the implementation of applicable security patches as required in R3.</u></p> <p><u>OR</u></p> <p><u>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.</u>The Responsible Entity did not document the implementation of applicable security patches as</p>

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>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, <u>as technically feasible</u> , 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, <u>as technically feasible</u> , 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, <u>as technically feasible</u> , 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, <u>as technically feasible</u> , 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, <u>as technically feasible</u> , documented and implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing <u>and installation</u> of the signatures.	The Responsible Entity, <u>as technically feasible</u> , 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, <u>as technically feasible</u> , 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, <u>as technically feasible</u> , 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. <u>N/A</u>	<u>The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.</u> The Responsible Entity documented and implemented	<u>The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.</u> The Responsible Entity implemented technical and	<u>The Responsible Entity did not document nor implemented technical and procedural controls that enforce access authentication of, and accountability for, all user activity.</u> The Responsible Entity did not document nor implement

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		technical and procedural controls that enforce access authentication and accountability, however those technical and procedural controls are not enforced for all user activity.	procedural controls that enforce access authentication but does not provided accountability for, all user activity.	technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
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.

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.
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	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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 personnel changes (for example, change in assignment or termination).	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 personnel changes (for example, change in assignment or termination).	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).
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 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. 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).

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.
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	The Responsible Entity established formal methods, processes, and	The Responsible Entity established formal methods, processes, and	The Responsible Entity did not establish formal methods,

Standard Number CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	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.	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.	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.	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 Security Perimeter.	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 Security Perimeter.	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 Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic 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.	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.

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.