

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 <b>or</b> 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><b>AND</b></p> <p>changes to the delegated authority are not documented within thirty calendar days of the effective date.</p>

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 <b>either</b> : 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 <b>both</b> : 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 <del>not</del> 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 <del>the Critical</del> 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 <b>but</b> 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 <b>has implemented but not documented</b> 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 <b>has documented but not implemented</b> 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"> <li>• 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.</li> <li>• 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.</li> <li>• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.</li> <li>• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.</li> </ul>	<p>or more of the following physical access methods:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.</li> <li>• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.</li> </ul>	<p>physical access methods:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.</li> <li>• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.</li> </ul>
R5.	N/A	<p>The Responsible Entity <b>has implemented but not documented</b> 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 <b>has documented but not implemented</b> 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 <b>has not documented nor implemented</b> 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 <b>has documented but not implemented</b> 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 <b>has not implemented nor documented</b> 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"> <li>• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or</li> <li>• 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.</li> </ul>	<p>method,</p> <ul style="list-style-type: none"> <li>• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or</li> <li>• 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, <b>but</b> 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.</li> </ul>	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> <li>• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or</li> <li>• 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.</li> </ul>	<p>access control and monitoring method,</p> <ul style="list-style-type: none"> <li>• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or</li> <li>• 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.</li> </ul>
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 <b>but</b> 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 <b>but</b> 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 <b>but</b> 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 <b>established (implemented) but did not document</b> a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity <b>documented but did not establish (implement)</b> 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 <b>but</b> 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 <b>established (implemented) but did not document</b> , 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 <b>documented but did not establish (implement)</b> , 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 <b>did not establish (implement) nor document</b> , 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 <b>but</b> 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 <b>but</b> 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 <b>but</b> 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 <b>nor</b> 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.