

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

This redline is showing the changes made between the balloted set of Version 1 VSLs and the proposed Version 2 VSLs.

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

**Index:**

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

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

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

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

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

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

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

| Standard Number CIP-004-2 — Personnel & Training   |  |   |  |   |
|--|--|---|--|---|
| R#   | Lower VSL  | Moderate VSL  | High VSL   | Severe VSL  |
| R2<br>(Proposed changes to align with version 2)   | The Responsible Entity established, <del>(implemented,)</del> 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, <del>(implement,)</del> 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, <del>(implement),</del> 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.<br>(Version 1)                               | At least one individual but less than 5% of personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.   | At least 5% but less than 10% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.   | At least 10% but less than 15% of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.   | 15% or more of all personnel having access to Critical Cyber Assets, including contractors and service vendors, were not trained within ninety calendar days of such authorization.   |
| R2.1<br>(Proposed changes to align with version 2) | At least one individual but less than 5% of personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained <b>prior to their being granted such access except in specified circumstances such as an emergency.</b> | At least 5% but less than 10% of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained <b>prior to their being granted such access except in specified circumstances such as an emergency.</b> | At least 10% but less than 15% of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained <b>prior to their being granted such access except in specified circumstances such as an emergency.</b> | 15% or more of all personnel having <u>authorized cyber or unescorted physical</u> access to Critical Cyber Assets, including contractors and service vendors, were not trained <b>prior to their being granted such access except in specified circumstances such as an emergency.</b> |

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

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

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

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

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

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

| Standard Number CIP-005-2 — Electronic Security Perimeter(s) |           |              |   |   |
|--|-----------|--------------|---|---|
| R#   | Lower VSL | Moderate VSL | High VSL  | Severe VSL  |
|  |           |              |   | Security Perimeter(s) where applicable.   |
| R2.3<br>(Proposed changes to align with version 2)           | N/A       | N/A          | <a href="#">The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.</a> | The Responsible Entity did not <b>implement</b> <b>nor</b> 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.<br>(Version 1)   | N/A       | N/A          | <p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created but did not maintain a physical security plan.</p>                        | The Responsible Entity did not create and maintain a physical security plan.                                 |
| R1<br>(Proposed changes to align with version 2)                       | N/A       | N/A          | <p>The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).</p> <p>OR</p> <p>The Responsible Entity created <b>and implemented</b> but did not maintain a physical security plan.</p> | The Responsible Entity did not <b>create and document, implement, and</b> maintain a physical security plan. |

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

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

| Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets |           |              |  |   |
|--|-----------|--------------|--|---|
| R#   | Lower VSL | Moderate VSL | High VSL   | Severe VSL  |
|  |           |              |  | Requirement <a href="#">R4</a> .  |
| R1.5<br>(Version 1)  | N/A       | N/A          | The Responsible Entity's physical security plan does not include either the procedures for reviewing access authorization requests or revocation of access authorization, in accordance with CIP-004 Requirement R4.   | The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.  |
| <b>R1.5</b><br>(Proposed changes to align with version 2)              | N/A       | N/A          | The Responsible Entity's physical security plan does not <del>include</del> <b>address</b> either the <del>procedures</del> <b>process</b> for reviewing access authorization requests or <del>the process</del> <b>for</b> revocation of access authorization, in accordance with CIP-004- <del>2</del> Requirement R4. | The Responsible Entity's physical security plan does not <del>include</del> <b>address the process</b> <del>procedures</del> for reviewing access authorization requests and <del>the process</del> <b>for</b> revocation of access authorization, in accordance with CIP-004- <del>2</del> Requirement R4. |
| R1.6<br>(Version 1)  | N/A       | N/A          | N/A  | The Responsible Entity's physical security plan does not include procedures for escorted access within the physical security perimeter.   |
| <b>R1.6</b><br>(Proposed changes to align with version 2)              | N/A       | N/A          | N/A  | The Responsible Entity's physical security plan does not <del>include</del> <b>procedures</b> <del>address the process</del> <b>for continuous</b> 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<br>(Version 1)  | N/A       | N/A          | The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration <b>but</b> the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.   | The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration.   |
| R1.7<br>(Proposed changes to align with version 2)                     | N/A       | N/A          | The Responsible Entity's physical security plan <del>includes</del> <b>addresses</b> a process for updating the physical security plan within <del>ninety</del> <b>thirty</b> calendar days of <b>the completion of</b> any physical security system redesign or reconfiguration <b>but</b> the plan was not updated within <del>90</del> <b>thirty</b> calendar days of <b>the completion of any</b> physical security system redesign or reconfiguration. | The Responsible Entity's physical security plan does not <del>include</del> <b>address</b> a process for updating the physical security plan within <del>ninety</del> <b>thirty</b> calendar days of <b>the completion of any</b> physical security system redesign or reconfiguration. |

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

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

| Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets |                          |  |  |   |
|--|--------------------------|--|--|---|
| R#   | Lower VSL                | Moderate VSL   | High VSL   | Severe VSL  |
|  |                          |  |  | more of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.   |
| New R2.1<br>(Proposed changes to align with version 2)                 | N/A (Rolled up into R2.) | N/A (Rolled up into R2.)   | N/A (Rolled up into R2.)   | N/A (Rolled up into R2.)  |
| New R2.2<br>(Proposed changes to align with version 2)                 | N/A (Rolled up into R2.) | N/A (Rolled up into R2.)   | N/A (Rolled up into R2.)   | N/A (Rolled up into R2.)  |
| R3<br>(Version 1)  | N/A                      | 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 at least one of the monitoring methods identified in | 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 at least one of the monitoring methods identified in | 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 at least one of the monitoring methods identified in Requirements R3.1 or R3.2. |

| Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets |  |   |   |   |
|--|--|---|---|---|
| R#   | Lower VSL  | Moderate VSL  | High VSL  | Severe VSL  |
|  |  | Requirements R3.1 or R3.2.  | Requirements R3.1 or R3.2.  | OR<br><br>One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.   |
| R3<br>(Proposed changes to align with version 2)                       | N/A  | N/A   | N/A   | A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.  |
| R4<br>(Version 1)  | The Responsible Entity <b>has implemented but not 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 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, <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. | 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 logging methods identified in Requirements R4.1, R4.2, or R4.3. | 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 logging methods identified in Requirements R4.1, R4.2, or R4.3. |

| Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets |           |  |  |   |
|--|-----------|--|--|---|
| R#   | Lower VSL | Moderate VSL   | High VSL   | Severe VSL  |
| R4<br>(Proposed changes to align with version 2)                       | N/A       | <p>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 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>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 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>The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:</p> <ul style="list-style-type: none"> <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> |

| Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets |           |  |  |   |
|--|-----------|--|--|---|
| R#   | Lower VSL | Moderate VSL   | High VSL   | Severe VSL  |
| R5<br>(Version 1)  | N/A       | N/A  | N/A  | The Responsible Entity did not retain electronic access logs for at least ninety calendar days.   |
| R5<br>(Proposed changes to align with version 2)                       | N/A       | 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 monitoring methods: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.</li> </ul> | 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 monitoring methods: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.</li> </ul> | 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: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.</li> </ul> <p>OR</p> <p>An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-</p> |

| Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets |   |   |   |   |
|--|---|---|---|---|
| R#   | Lower VSL   | Moderate VSL  | High VSL  | Severe VSL  |
|  |   |   |   | 008-2.  |
| R6<br>(Version 1)  | The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly <b>but</b> the program does not include one of the requirements R6.1, R6.2, and R6.3.   | The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly <b>but</b> the program does not include two of the requirements R6.1, R6.2, and R6.3.   | The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly <b>but</b> the program does not include any of the requirements R6.1, R6.2, and R6.3.   | The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.  |
| R6<br>(Proposed changes to align with version 2)                       | The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:<br><ul style="list-style-type: none"> <li>• Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method,</li> <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</li> </ul> | 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:<br><ul style="list-style-type: none"> <li>• Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method,</li> <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</li> </ul> | 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:<br><ul style="list-style-type: none"> <li>• Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method,</li> <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</li> </ul> | 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:<br><ul style="list-style-type: none"> <li>• Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method,</li> <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</li> </ul> |

| Standard Number CIP-006-2 — Physical Security of Critical Cyber Assets |   |   |   |  |
|--|---|---|---|--|
| R#   | Lower VSL   | Moderate VSL  | High VSL  | Severe VSL   |
|  | of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. | security or other personnel authorized to control and monitor physical access as specified in Requirement R4, <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. | physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.   | physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.                                    |
| New R7<br>(Proposed changes to align with version 2)                   | <u>The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.</u>   | <u>The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.</u>   | <u>The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.</u>   | <u>The Responsible Entity retained physical access logs for less than 45 calendar days.</u>  |
| New R8<br>(Proposed changes to align with version 2)                   | The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly <b>but</b> the program does not include one of the Requirements R8.1, R8.2, and R8.3.   | The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly <b>but</b> the program does not include two of the Requirements R8.1, R8.2, and R8.3.                           | The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly <b>but</b> the program does not include any of the Requirements R8.1, R8.2, and R8.3. | The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. |
| New R8.1<br>(Proposed changes to align with version 2)                 | N/A (Rolled up into R8.)  | N/A (Rolled up into R8.)  | N/A (Rolled up into R8.)  | N/A (Rolled up into R8.)   |

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

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

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

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

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

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

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

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

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