

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

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

Index:

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

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

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

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

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

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

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

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

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