

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-002-2 through CIP-009-2 to CIP-002-3 through CIP-009-3.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 3 CIP-002-3 thru CIP-009-32 Standards:

Index:

Standard Number CIP-003-3 Security Management Controls2
Standard Number CIP-006-3a Physical Security of Critical Cyber Assets3

| Standard Number CIP-003 — Security Management Controls | | | |
|--|--------------------|---|-----------------------|
| Standard Number | Requirement Number | Text of Requirement | Violation Risk Factor |
| CIP-003-3 | R2.3. | Where allowed by Standards CIP-002-3 through CIP-009-3, 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 |

| Standard Number CIP-006 — Physical Security of Critical Cyber Assets | | | |
|--|--------------------|---|-----------------------|
| Standard Number | Requirement Number | Text of Requirement | Violation Risk Factor |
| CIP-006-2 | R1.5. | Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4. | MEDIUM |
| CIP-006-3a | R1.6 | A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following components: | MEDIUM |
| CIP-006-3a | R1.6.1 | Visitor logs (manual or automated) to document the visitor’s identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort. | MEDIUM |
| CIP-006-3a | R1.6.2 | Requirement for continuous escorted access within the Physical Security Perimeter of visitors. | MEDIUM |
| CIP-006-2 | R2.2. | Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3. | MEDIUM |
| CIP-006-2 | R5. | <p>Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:</p> <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. | MEDIUM |
| CIP-006-2 | R7. | Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance | LOWER |

| Standard Number CIP-006 — Physical Security of Critical Cyber Assets | | | |
|--|--------------------|--|-----------------------|
| Standard Number | Requirement Number | Text of Requirement | Violation Risk Factor |
| | | with the requirements of Standard CIP-008-3. | |