

**Violation Risk Factors — Version 1 Standards Pre-ballot Matrix**

The following table lists the Violation Risk Factors (VRFs) for the requirements in the following Version 1 Critical Infrastructure Protection standards:

- CIP-002-1 — Critical Cyber Asset Identification
- CIP-003-1 — Security Management Controls
- CIP-004-1 — Personnel & Training
- CIP-005-1 — Electronic Security Perimeter(s)
- CIP-006-1 — Physical Security of Critical Cyber Assets
- CIP-007-1 — Systems Security Management
- CIP-008-1 — Incident Reporting and Response Planning
- CIP-009-1 — Recovery Plans for Critical Cyber Assets

These VRFs are the weighted average of the stakeholder VRF selections from the second posting of the Version 1 VRF survey.

<b>CIP-002-1 — Critical Cyber Asset Identification</b>			
CIP-002-1	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	LOWER
CIP-002-1	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	LOWER
CIP-002-1	R1.2.	The risk-based assessment shall consider the following assets:	LOWER
CIP-002-1	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	LOWER
CIP-002-1	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.4.	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	LOWER
CIP-002-1	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	LOWER
CIP-002-1	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.7.	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	LOWER
CIP-002-1	R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	LOWER
CIP-002-1	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible	MEDIUM

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-002-1 — Critical Cyber Asset Identification</b>			
		Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	
CIP-002-1	R3.1.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	
CIP-002-1	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	LOWER
CIP-002-1	R3.3.	The Cyber Asset is dial-up accessible.	LOWER
CIP-002-1	R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	LOWER

<b>CIP-003-1 — Security Management Controls</b>			
CIP-003-1	R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	LOWER
CIP-003-1	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.	LOWER
CIP-003-1	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	LOWER
CIP-003-1	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-1	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-003-1	R2.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	LOWER
CIP-003-1	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-1	R2.3.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-1	R3.	Exceptions — Instances where the Responsible Entity cannot	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-003-1 — Security Management Controls</b>			
		conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	
CIP-003-1	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	LOWER
CIP-003-1	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	LOWER
CIP-003-1	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	LOWER
CIP-003-1	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	LOWER
CIP-003-1	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	
CIP-003-1	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	LOWER
CIP-003-1	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	LOWER
CIP-003-1	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-1	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	LOWER
CIP-003-1	R5.1.1.	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	LOWER
CIP-003-1	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	
CIP-003-1	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	LOWER
CIP-003-1	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-1	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-003-1 — Security Management Controls</b>			
		change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	

<b>CIP-004-1 — Personnel &amp; Training</b>			
CIP-004-1	R1.	Awareness — The Responsible Entity shall establish, maintain, and 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 program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: - Direct communications (e.g., emails, memos, computer based training, etc.); - Indirect communications (e.g., posters, intranet, brochures, etc.); - Management support and reinforcement (e.g., presentations, meetings, etc.).	LOWER
CIP-004-1	R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	LOWER
CIP-004-1	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	LOWER
CIP-004-1	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	LOWER
CIP-004-1	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-1	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	
CIP-004-1	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	
CIP-004-1	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	LOWER
CIP-004-1	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	LOWER
CIP-004-1	R3.	Personnel Risk Assessment —The Responsible Entity shall 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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	LOWER
CIP-004-1	R3.1.	The Responsible Entity shall ensure that each assessment	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-004-1 — Personnel &amp; Training</b>			
		conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	
CIP-004-1	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	LOWER
CIP-004-1	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.	LOWER
CIP-004-1	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	LOWER
CIP-004-1	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	LOWER
CIP-004-1	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	LOWER

<b>CIP-005-1 — Electronic Security Perimeter(s)</b>			
CIP-005-1	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	MEDIUM
CIP-005-1	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	LOWER
CIP-005-1	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	LOWER
CIP-005-1	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-005-1 — Electronic Security Perimeter(s)</b>			
CIP-005-1	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	LOWER
CIP-005-1	R1.5.	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a 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.	
CIP-005-1	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	LOWER
CIP-005-1	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	LOWER
CIP-005-1	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	MEDIUM
CIP-005-1	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	MEDIUM
CIP-005-1	R2.3.	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-1	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	LOWER
CIP-005-1	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-1	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-1	R2.5.2.	The authentication methods.	LOWER
CIP-005-1	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.	LOWER
CIP-005-1	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-1	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-005-1 — Electronic Security Perimeter(s)</b>			
CIP-005-1	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	LOWER
CIP-005-1	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	LOWER
CIP-005-1	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	LOWER
CIP-005-1	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	LOWER
CIP-005-1	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-1	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	LOWER
CIP-005-1	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	LOWER
CIP-005-1	R4.5.	A review of controls for default accounts, passwords, and network management community strings; and,	LOWER
CIP-005-1	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	LOWER
CIP-005-1	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	LOWER
CIP-005-1	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.	LOWER
CIP-005-1	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	LOWER
CIP-005-1	R5.3.	The Responsible Entity shall retain electronic 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.	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-006-1 — Physical Security of Critical Cyber Assets</b>			
CIP-006-1	R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-1	R1.1.	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also 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 the Critical Cyber Assets.	MEDIUM
CIP-006-1	R1.2.	Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-1	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-1	R1.4.	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-1	R1.5.	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	LOWER
CIP-006-1	R1.6.	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-1	R1.7.	Process for updating the physical security plan within ninety calendar days 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-006-1	R1.8.	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	LOWER
CIP-006-1	R1.9.	Process for ensuring that the physical security plan is reviewed at least annually.	LOWER
CIP-006-1	R2.	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:	MEDIUM
CIP-006-1	R2.1.	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.	MEDIUM
CIP-006-1	R2.2.	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.	MEDIUM

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-006-1 — Physical Security of Critical Cyber Assets</b>			
CIP-006-1	R2.3.	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	MEDIUM
CIP-006-1	R2.4.	Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	MEDIUM
CIP-006-1	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. One or more of the following monitoring methods shall be used:	MEDIUM
CIP-006-1	R3.1.	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.	MEDIUM
CIP-006-1	R3.2.	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.	LOWER
CIP-006-1	R4.	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:	LOWER
CIP-006-1	R4.1.	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	LOWER
CIP-006-1	R4.2.	Video Recording: Electronic capture of video images of sufficient quality to determine identity.	LOWER
CIP-006-1	R4.3.	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 R2.3.	LOWER
CIP-006-1	R5.	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.	LOWER
CIP-006-1	R6.	Maintenance and Testing — The Responsible Entity shall implement maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-1	R6.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	LOWER
CIP-006-1	R6.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-006-1 — Physical Security of Critical Cyber Assets</b>			
CIP-006-1	R6.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER

<b>CIP-007-1 — Systems Security Management</b>			
CIP-007-1	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	MEDIUM
CIP-007-1	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	LOWER
CIP-007-1	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-1	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-1	R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	LOWER
CIP-007-1	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MEDIUM
CIP-007-1	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	MEDIUM
CIP-007-1	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER
CIP-007-1	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document 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).	LOWER
CIP-007-1	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	LOWER
CIP-007-1	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER
CIP-007-1	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-007-1 — Systems Security Management</b>			
		malware on all Cyber Assets within the Electronic Security Perimeter(s).	
CIP-007-1	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER
CIP-007-1	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.	LOWER
CIP-007-1	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	LOWER
CIP-007-1	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.	
CIP-007-1	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	LOWER
CIP-007-1	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	LOWER
CIP-007-1	R5.1.3.	The Responsible Entity shall 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.	LOWER
CIP-007-1	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	LOWER
CIP-007-1	R5.2.1	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	LOWER
CIP-007-1	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-1	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	LOWER
CIP-007-1	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-1	R5.3.1	Each password shall be a minimum of six characters.	LOWER
CIP-007-1	R5.3.2	Each password shall consist of a combination of alpha, numeric,	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-007-1 — Systems Security Management</b>			
		and “special” characters.	
CIP-007-1	R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.	
CIP-007-1	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	LOWER
CIP-007-1	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	LOWER
CIP-007-1	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	LOWER
CIP-007-1	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.	LOWER
CIP-007-1	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-1	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-1	R7.	Disposal or Redeployment — The Responsible Entity shall 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.	
CIP-007-1	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-1	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-1	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-1	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	LOWER
CIP-007-1	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-1	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	LOWER
CIP-007-1	R8.3.	A review of controls for default accounts; and,	LOWER
CIP-007-1	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-007-1 — Systems Security Management</b>			
CIP-007-1	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	LOWER

<b>CIP-008-1 — Incident Reporting and Response Planning</b>			
CIP-008-1	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	LOWER
CIP-008-1	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER
CIP-008-1	R1.2.	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	LOWER
CIP-008-1	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.	LOWER
CIP-008-1	R1.4.	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	LOWER
CIP-008-1	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-1	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-1	R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	LOWER

<b>CIP-009-1 — Recovery Plans for Critical Cyber Assets</b>			
CIP-009-1	R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	MEDIUM
CIP-009-1	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	MEDIUM
CIP-009-1	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-1	R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	LOWER
CIP-009-1	R3.	Change Control — Recovery plan(s) shall be updated to reflect	LOWER

<b>CIP-009-1 — Recovery Plans for Critical Cyber Assets</b>			
		any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	
CIP-009-1	R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	LOWER
CIP-009-1	R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	LOWER