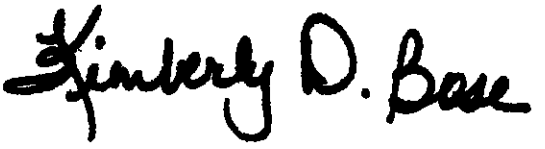
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Mandatory Reliability Standards for the Bulk-Power System — Docket No. RM06-22-008

ERRATA NOTICE

(March 23, 2010)

On March 18, 2010, the Commission issued an "Order Addressing Violation Severity Level Assignments For Critical Infrastructure Protection Reliability Standards," in the above-referenced proceeding. *Mandatory Reliability Standards for Critical Infrastructure Protection,* 130 FERC ¶ 61,211 (2010). In this order, the Commission approved the proposed Violation Severity Level assignments, with revisions as indicated in the Appendix. The Appendix issued did not contain the revisions in redline. This errata notice corrects the Appendix to show the redline changes in the attached Appendix.



Kimberly D. Bose,
Secretary.

Appendix

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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:	MED	N/A	N/A	~~The Responsible Entity has documented but not implemented a cyber security policy.~~	The Responsible Entity has not documented or ~~nor~~ implemented a cyber security policy.	CIP Guideline 2 VSL Guideline 2(b)
CIP-003-1	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOW	N/A	N/A	~~The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.~~	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annually review and ~~nor~~ approvale of its cyber security policy.	CIP Guideline 2 VSL Guideline 2(b)
CIP-003-1	R2.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	LOW	N/A	~~The senior manager is identified by name, title, and date of designation but the designation is missing business phone or business address~~	The senior manager is identified by name, title, and date of designation but the designation is missing business phone or business address ~~The senior manager is identified by business phone and business address but the designation is missing one of the following: name, title, or date of designation~~	Identification of the senior manager is missing one of the following: name, title, or date of designation. ~~The senior manager is not identified by name, title, business phone, business address, and date of designation.~~	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-003-1	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOW	~~Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.~~	~~Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.~~	~~Changes to the senior manager were documented in days of the effective date.~~	Changes to the senior manager were not documented within 30~~in 120 or more~~ days of the effective date.	VSL Guideline 1
CIP-003-1	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	LOW	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy ~~(pertaining to CIP 002 through CIP 009)~~, in R1, exceptions were documented, **but** were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy ~~(pertaining to CIP 002 through CIP 009)~~, in R1, exceptions were not documented. ~~and were not authorized by the senior manager or delegate(s).~~	VSL Guideline 2(b)
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).	LOW	~~Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).~~	~~Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).~~	~~Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).~~	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 ~~in 120 or more~~ days of being approved by the senior manager or delegate(s).	VSL Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	N/A	N/A	~~The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) in R1, but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.~~	The Responsible Entity has a documented exception to the cyber security policy ~~(pertaining to CIP 002 through CIP 009)~~ in R1, but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.	VSL Guideline 2(b)
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.	LOW	N/A	N/A	~~Exceptions to the cyber security policy (pertaing to CIP 002 through CIP 009)were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.~~	Exceptions to the cyber security policy ~~(pertaining to CIP 002 through CIP 009)~~ were not reviewed ~~nor~~ or were not approved ~~annually~~ on an annual basis by the senior manager or delegate(s) to ensure the exceptions are still required and valid or the review and approval is not documented.	CIP Guideline 2 VSL Guideline 2(b)
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.	MED	N/A	~~The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.~~	~~The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.~~	The Responsible Entity did not implement or ~~nor~~ did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	N/A	~~The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.~~	~~The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.~~	The Responsible Entity did not annually~~,~~ assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, ~~nor~~ OR The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.	VSL Guideline 2(b)
CIP-003-1	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOW	N/A	~~The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.~~	~~The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information..~~	The Responsible Entity did not implement or ~~nor~~ did not document a program for managing access to protected Critical Cyber Asset information.	CIP Guideline 2 VSL Guideline 2(b)
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.	LOW	N/A	N/A	The Responsible Entity did identify the personnel by name, title, ~~business phone but did not identify~~ and the information for which they are responsible for authorizing access, but the business phone is missing.	Personnel are not identified by name, title, or the information for which they are responsible for authorizing access. ~~The Responsible Entity did not identify the personnel by name, title, business phone nor the information for which they are responsible for authorizing access.~~	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-003-1	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of 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.	LOW	~~The Responsible Entity has established but not documented a change control process~~ ~~OR~~ ~~The Responsible Entity has established but not documented a configuration management process.~~	~~The Responsible Entity has established but not documented both a change control process and configuration management process.~~	~~The Responsible Entity has not established and documented a change control process~~ ~~OR~~ ~~The Responsible Entity has not established and documented a configuration management process~~	The Responsible Entity has not established ~~and~~ or documented a change control process for the activities required in R6, ~~OR~~AND The Responsible Entity has not established ~~and~~ or documented a configuration management process for the activities required in R6.	CIP Guideline 2 VSL Guideline 2(b)
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.	MED	~~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~~N/A	~~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.~~ N/A	~~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.~~ N/A	~~15% or more of~~ Not all personnel having access to Critical Cyber Assets, including contractors and service vendors, were ~~not~~ trained within ninety calendar days of such authorization.	CIP Guideline 1
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:	MED	N/A	~~The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.~~	~~The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4~~.	The training does not include ~~three~~ one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-004-1	R2.2.1.	The proper use of Critical Cyber Assets;	LOW	N/A	N/A	N/A	N/A	
CIP-004-1	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOW	N/A	N/A	N/A	N/A	
CIP-004-1	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	MED	N/A	N/A	N/A	N/A	
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.	MED	N/A	N/A	N/A	N/A	
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.	LOW	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include ~~either the date the training was completed or~~ attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed ~~or~~ and attendance records.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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:	MED	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~~ as stated in R3, 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 more than thirty (30) days 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~~as stated in R3, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.	VSL Guideline 2(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).	MED	~~The Responsible Entity did not document one or more access points to the electronic security perimeter(s).~~	~~The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).~~	~~The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter.~~ ~~OR~~ ~~The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).~~	The Responsible Entity did not ensure that every ~~one or more~~ Critical Cyber Assets resides within an Electronic Security Perimeter, ~~and~~OR the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) ~~for all Critical Cyber Assets~~.	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	MED	N/A	~~One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.~~	~~One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005~~	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified ~~and~~ OR is not protected pursuant to the requirements of Standard CIP-005.	CIP Guideline 1 VSL Guideline 2(b)
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.	MED	~~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)~~ in one (1) 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.	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	N/A	N/A	~~The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.~~	The Responsible Entity did not maintain documentation of ~~two~~ one or more of the following: Electronic Security Perimeter(s), interconnected Critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.	CIP Guideline 1
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).	MED	N/A	~~The Responsible Entity implemented but did not 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).~~	~~The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).~~	The Responsible Entity did not implement or ~~nor~~ did not 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).	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	MED	N/A	~~At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security Perimeter.~~	~~At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.~~	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, ~~and~~ or did not document, individually or by specified grouping, the configuration of those ports and services.	CIP Guideline 1 VSL Guideline 2(b)
CIP-005-1	R2.5.	The required documentation shall, at least, identify and describe:	LOW	~~The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4~~	~~The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4~~	~~The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4~~	The required documentation for R2 did not include one or more~~any~~ of the elements described in R2.5.1 through R2.5.4	CIP Guideline 1 CIP Guideline 2
CIP-005-1	R2.5.1.	The processes for access request and authorization.	LOW	N/A	N/A	N/A	N/A	
CIP-005-1	R2.5.2.	The authentication methods.	LOW	N/A	N/A	N/A	N/A	
CIP-005-1	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.	LOW	N/A	N/A	N/A	N/A	
CIP-005-1	R2.5.4.	The controls used to secure dial-up accessible connections.	LOW	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	MED	~~The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.~~	~~The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.~~	~~The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.~~	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging at ~~15% or more of the~~ access points.	CIP Guideline 1 CIP Guideline 2 VSL Guideline 2(b)
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.	MED	~~The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices.~~ ~~OR~~ ~~Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.~~	~~Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.~~	~~Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.~~	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at ~~15% or more of the~~ one or more access points to dial-up devices.	CIP Guideline 1 CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	MED	N/A	N/A	~~Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate notification to designated response personnel.~~	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR the above alerts do not provide for appropriate notification to designated response personnel. OR Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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:	MED	~~The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).~~	The Responsible Entity did not perform a Vulnerability Assessment at least annually for~~15%~~ one or more of the access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.	CIP Guideline 1
CIP-005-1	R4.1.	A document identifying the vulnerability assessment process;	LOW	N/A	N/A	N/A	N/A	
CIP-005-1	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MED	N/A	N/A	N/A	N/A	
CIP-005-1	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MED	N/A	N/A	N/A	N/A	
CIP-005-1	R4.4.	A review of controls for default accounts, passwords, and network management community strings; and,	MED	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	MED	N/A	N/A	N/A	N/A	
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.	LOW	~~For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.~~	~~For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.~~	~~For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.~~	~~For 15% or more of the applicable changes, t~~The Responsible Entity did not update ~~the~~ documentation to reflect ~~the~~ a modification of the network or controls within ninety calendar days of the change.	CIP Guideline 1
CIP-006-1	R1.5.	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	MED	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~~ or does not include revocation of access authorization, in accordance with CIP-004 Requirement R4.	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	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 but 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. OR The plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	VSL Guideline 2(b)
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.	LOW	~~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~~ afforded one (1)~~(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.	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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:	MED	N/A	~~The Responsible Entity has implemented but not documented 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 documented but not 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.~~	The Responsible Entity has not documented, or has not ~~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.	CIP Guideline 2 VSL Guideline 2(b)
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.	MED	N/A	N/A	N/A	N/A	
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.	MED	N/A	N/A	N/A	N/A	
CIP-006-1	R2.3.	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	MED	N/A	N/A	N/A	N/A	
CIP-006-1	R2.4.	Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	MED	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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:	MED	N/A	~~The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twentyfour hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.~~	~~The Responsible Entity has~~ **documented ~~but not~~ implemented ~~the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twentyfour hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2.~~**	The Responsible Entity **has not documented or has not ~~nor~~ implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twentyfour hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2. OR One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.	CIP Guideline 2 VSL Guideline 2(b)
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.	MED	N/A	N/A	N/A	N/A	
CIP-006-1	R3.2.	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.	LOW	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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:	LOW	~~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 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, but 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 has documented but not 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.~~	The Responsible Entity **has not implemented or has not nor 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 logging methods identified in Requirements R4.1, R4.2, or R4.3 or has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	CIP Guideline 2 VSL Guideline 2(b)
CIP-006-1	R4.1.	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	LOW	N/A	N/A	N/A	N/A	
CIP-006-1	R4.2.	Video Recording: Electronic capture of video images of sufficient quality to determine identity.	LOW	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	N/A	N/A	N/A	N/A	
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:	MED	~~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 but 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 but 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 but the program does not include any one or more 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. OR The implemented program does not include one or more of the requirements; R6.1, R6.2, and R6.3.	CIP Guideline 1
CIP-006-1	R6.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MED	N/A	N/A	N/A	N/A	
CIP-006-1	R6.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	LOW	N/A	N/A	N/A	N/A	
CIP-006-1	R6.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOW	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	MED	N/A	~~The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, but did not document that testing is performed as required in R1.2.~~ ~~OR~~ ~~The Responsible Entity did not document the test results as required in R1.3.~~	~~The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.~~	~~The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1,~~ ~~AND~~ ~~The Responsible Entity did not document that testing was performed as required in R1.2~~ ~~AND~~ ~~The Responsible Entity did not document the test results as required in R1.3.~~ The Responsible Entity did not ensure the prevention of adverse affects described in R1, by not including the required minimum significant changes, OR The Responsible Entity did not address one or more of the following: R1.1, R1.2, R1.3.	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	MED	N/A	N/A	N/A	N/A	
CIP-007-1	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOW	N/A	N/A	N/A	N/A	
CIP-007-1	R1.3.	The Responsible Entity shall document test results.	LOW	N/A	N/A	N/A	N/A	
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.	MED	N/A	~~The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	~~The Responsible Entity documented but did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	The Responsible Entity did not establish or ~~nor~~did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	CIP Guideline 2 VSL Guideline 2(b)
CIP-007-1	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MED	~~The Responsible entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security perimeter(s).~~	~~The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	The Responsible Entity enabled one or more ports or ~~and~~ services not required for normal and emergency operations on ~~15% or more of the~~ Cyber Assets inside the Electronic Security Perimeter(s).	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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).	MED	~~The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	The Responsible Entity did not disable one or more other ports ~~and~~ or services, including those used for testing purposes, prior to production use for ~~15% or more of the~~ Cyber Assets inside the Electronic Security Perimeter(s).	CIP Guideline 1 VSL Guideline 2(b)
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).	LOW	~~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 but 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 established but did not document, 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 documented but did not establish, 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 **did not establish or did not** ~~nor~~ document, 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)	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	~~The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.~~	~~The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.~~	~~The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.~~	The Responsible Entity did not documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30~~120~~ calendar days ~~or more~~ after the availability of the patches and upgrades.	VSL Guideline 1
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 malware on all Cyber Assets within the Electronic Security Perimeter(s).	MED	~~The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).~~	~~The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).~~	~~The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).~~	The Responsible Entity, ~~as~~ where technically feasible, did not use anti-virus software ~~and~~ or other malicious software ("malware") prevention tools, ~~nor implemented compensating measures~~, on one ~~15%~~ or more Cyber Assets within the Electronic Security Perimeter(s).	CIP Guideline 1 VSL Guideline 2(b)
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.	MED	~~The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.~~	~~The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."~~	~~The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."~~	The Responsible Entity, ~~as technically feasible, did not document nor~~ or did not implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.		N/A	~~The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.~~	~~The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.~~	The Responsible Entity did not document or did not ~~nor~~ implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	CIP Guideline 2 VSL Guideline 2(b)
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.	LOW	~~At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.~~	~~One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.~~	~~Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.~~	~~Five (5) % or more of~~ One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.	CIP Guideline 1 VSL Guideline 2(b)
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).	MED	N/A	~~Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).~~	~~Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination)~~	Where such accounts must be shared, the Responsible Entity ~~does not have~~ has not implemented (one or more components of) 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).	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOW	~~The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.~~	~~The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.~~	~~The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.~~	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2., R5.3.3 . **or** **does not~~nor~~ use passwords** subject to ~~as required in~~ R5.3.1, R5.3.2., R5.3.3 ~~and did not demonstrate why it is not technically feasible~~.	CIP Guideline 1 VSL Guideline 2(b)
CIP-007-1	R5.3.1	Each password shall be a minimum of six characters.	LOW	N/A	N/A	N/A	N/A	
CIP-007-1	R5.3.2	Each password shall consist of a combination of alpha, numeric, and "special" characters.	LOW	N/A	N/A	N/A	N/A	
CIP-007-1	R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.	MED	N/A	N/A	N/A	N/A	
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.	LOW	~~The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).~~	The Responsible Entity as technically feasible, did not implement automated tools or organizational process controls, ~~as technically feasible~~, to monitor system events that are related to cyber security on one ~~for 15~~% or more of Cyber Assets inside the Electronic Security Perimeter(s).	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	MED	N/A	~~The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.~~	~~The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.~~	The Responsible Entity **did not implement** or **did not ~~nor~~ document** the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	CIP Guideline 2 VSL Guideline 2(b)
CIP-007-1	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOW	~~The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.~~	~~The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.~~	~~The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.~~	The Responsible Entity did not retain one or more of the ~~any~~ logs specified in Requirement R6 for at least 90 calendar days.	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	~~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 but 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 but 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 but did not address redeployment ~~disposal~~ as specified in R7.2~~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. OR 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 but did not address disposal as specified in R7.1.. OR did not maintain records pertaining to disposal or redeployment as specified in R7.3 .	VSL Guideline 2(b)
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.	LOW	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	N/A	N/A	N/A	N/A	
CIP-007-1	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOW	N/A	N/A	N/A	N/A	
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:	LOW	~~The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.~~	~~The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.~~	~~The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.~~	The Responsible Entity did not performed ~~at least annually~~ a Vulnerability Assessment ~~for 85% or less of~~ on one or more Cyber Assets within the Electronic Security Perimeter at least annually. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.	CIP Guideline 1
CIP-007-1	R8.1.	A document identifying the vulnerability assessment process;	LOW	N/A	N/A	N/A	N/A	
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;	MED	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R8.3.	A review of controls for default accounts; and,	MED	N/A	N/A	N/A	N/A	
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.	MED	N/A	N/A	N/A	N/A	
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:	LOW	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 that ~~includes~~addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with R1.4 or R1.5. ~~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 that addresses all components of the sub-requirements R1.1 through R1.6.	VSL Guideline 2(b)
CIP-008-1	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOW	N/A	N/A	N/A	N/A	
CIP-008-1	R1.2.	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	LOW	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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.	LOW	N/A	N/A	N/A	N/A	
CIP-008-1	R1.4.	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	LOW	N/A	N/A	N/A	N/A	
CIP-008-1	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOW	N/A	N/A	N/A	N/A	
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.	LOW	N/A	N/A	N/A	N/A	
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.	LOW	~~The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for two but less than three calendar years.~~	~~The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than two calendar years.~~	~~The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than one calendar year.~~	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
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:	MED	N/A	~~The Responsible Entity has not annually reviewed recovery plan(s) for Critical Cyber Assets.~~	~~The Responsible Entity has created recovery plan(s) for Critical Cyber Assets but did not address one of the requirements CIP- 009-1 R1.1 or R1.2.~~	The Responsible Entity has not created or has not annually reviewed their recovery plan(s) for Critical Cyber Assets OR has created a plan but did not ~~that~~ address ~~at a minimum both~~ one or more of the requirements CIP- 009-1 R1.1 **and** R1.2.	VSL Guideline 2(b)
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).	MED	N/A	N/A	N/A	N/A	
CIP-009-1	R1.2.	Define the roles and responsibilities of responders.	MED	N/A	N/A	N/A	N/A	

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-009-1	R3.	Change Control — Recovery plan(s) shall be updated to reflect 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.	LOW	~~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.~~ N/A	~~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.~~ N/A	~~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.~~ N/A	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were not communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~in more than 180~~ 90 calendar days of the change.	VSL Guideline 1