UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC	**)**	**Docket Nos. RD10-6-000,**
RELIABILITY CORPORATION	**)**	**RD09-7-002**
	)	

COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO JANUARY 20, 2011 ORDER ON VIOLATION RISK FACTORS AND VIOLATION SEVERITY LEVELS FOR CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability
Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and
Critical Infrastructure Protection
North American Electric Reliability
Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

March 21, 2011

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC"), in compliance with the directive in the Federal Energy Regulatory Commission's ("FERC" or the "Commission") January 20, 2011 Order ("January 20 Order"),[1] directing NERC's to file complete sets of Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") to the Version 2 and Version 3 Critical Infrastructure Protection ("CIP") Standards, hereby submits this compliance filing that includes the following:

- A redline of the VRFs and VSLs for the CIP Version 2 Reliability Standards that includes the FERC-approved VRFs and VSLs for CIP Version 2 plus the directed modifications from the January 20, 2011 Order **(Exhibit B)**;

- A redline of the VRFs and VSLs for the CIP Version 3 Reliability Standards that includes the FERC-approved VRFs and VSLs for CIP Version 3 plus the directed modifications from the January 20, 2011 Order **(Exhibit C)**;

- A redline of the VRFs and the VSLs for the CIP Version 4 Reliability Standards carried over from the CIP Versions 2 and 3 VRFs and VSLs proposed in this filing for approval **(Exhibit D)**. NERC is requesting that the CIP Version 4 VRFs and VSLs included in this filing replace the proposed CIP Version 4 VRFs and VSLs included in NERC's February 10, 2011 Petition for Approval of the CIP Version 4 Reliability Standards;[2] and

- The complete set of FERC-approved VRFs and VSLs for CIP Version 1 **(Exhibit A)** is included for reference.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook*
Senior Vice President and General Counsel

Holly A. Hawkins*
Assistant General Counsel for Standards and
Critical Infrastructure Protection
North American Electric Reliability

[1] *Order on Version 2 and Version 3 Violation Risk Factors and Violation Severity Levels for Critical Infrastructure Protection Reliability Standards*, 134 FERC ¶ 61,045 (January 20, 2011).
[2] *Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection (CIP) Reliability Standards Version 4*, Docket No. RM06-22-000 (February 10, 2011)

North American Electric Reliability
Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

*Persons to be included on the
Commission's official service list.

III. REVISIONS TO CIP VIOLATION RISK FACTORS AND CIP VIOLATION SEVERITY LEVELS

On December 18, 2009, NERC filed a petition requesting FERC approval of proposed VRFs and VSLs for the CIP Version 2 Reliability Standards.[3] On December 29, 2009, NERC filed a petition for approval of the proposed VRFs and VSLs for the CIP Version 3 Reliability Standards.[4] FERC's January 20 Order approved the VRFs and VSLs for the CIP Versions 2 and 3 Standards, and directed modifications to be filed by March 21, 2011.

On February 10, 2011, NERC filed a petition for approval of the CIP Version 4 Standards that carried over the VRFs and VSLs from Versions 2 and 3 to Version 4.[5] Due to the short amount of time between the issuance of FERC's January 20 Order and NERC's February 10 filing, the VRFs and VSLs included in NERC's CIP Version 4 petition did not take into consideration the changes directed in the Commission's January 20 Order.

NERC staff has prepared a comprehensive set of VRFs and VSLs for CIP Versions 2, 3, and 4 based on the VRFs and VSLs approved in the January 20 Order. The comprehensive set

[3] *Petition of the North American Electric Reliability Corporation for Approval of Violation Severity Levels to Critical Infrastructure Protection (CIP) Version 2 Reliability Standards CIP-002-2 through CIP-009-2 And Violation Risk Factors For CIP-003-2 and CIP-006-2,* Docket Nos. RM06-22-000 and RD09-7-000 (December 18, 2009)

[4] *Compliance Filing of the North American Electric Reliability Corporation in Response to the Federal Energy Regulatory Commission's September 30, 2009 Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing,* Docket No. RD09-7-000 (December 29, 2009)

[5] *Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection (CIP) Reliability Standards Version 4,* Docket No. RM06-22-000 (February 10, 2011)

also includes the directed changes from the January 20 Order as well as minor, conforming changes. Accordingly, NERC hereby submits this compliance filing in response to the January 20 Order modifying the VRFs and VSLs for CIP Version 2 and 3 based on the guidance provided by the Commission on January 20. NERC also requests that the proposed CIP Version 4 VRFs and VSLs included in this filing replace the proposed CIP Version 4 VRFs and VSLs included in NERC's February 10, 2011 Petition for Approval of the CIP Version 4 Reliability Standards. The VRFs and VSLs included herein for Commission approval were approved by NERC's Board of Trustees on March 10, 2011.

V. CONCLUSION

The North American Electric Reliability Corporation respectfully requests that the Commission accept this Compliance Filing in accordance with the Commission's directives in the January 20, 2011 Order.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

/s/ Holly A. Hawkins
Holly A. Hawkins
Assistant General Counsel for Standards
and Critical Infrastructure Protection
North American Electric Reliability
Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 21st day of March, 2011.

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric
Reliability Corporation

EXHIBIT A

CIP VIOLATION RISK FACTORS AND VIOLATION SEVERITY LEVELS – VERSION 1

CIP Version 1 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-001-1	R1.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	N/A	N/A	The responsible entity has procedures for the recognition of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection but does not have a procedure for making their operating personnel aware of said events.	The responsible entity failed to have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.
CIP-001-1	R2.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	N/A	N/A	The responsible entity has demonstrated the existence of a procedure to communicate information concerning sabotage events, but not all of the appropriate parties in the interconnection are identified.	The responsible entity failed to have a procedure for communicating information concerning sabotage events.
CIP-001-1	R3.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall	N/A	The responsible entity has demonstrated the existence of a response guideline	The responsible entity has demonstrated the existence of a response guideline	The responsible entity failed to have a response guideline for reporting disturbances due to sabotage events.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.		for reporting disturbances due to sabotage events, but the guideline did not list all of the appropriate personnel to contact.	for reporting disturbances due to sabotage events, including all of the appropriate personnel to contact, but the guideline was not available to its operating personnel.	
CIP-001-1	R4.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	N/A	N/A	The responsible entity has established communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, but has not developed a reporting procedure.	The responsible entity failed to establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, nor developed a reporting procedure.
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.	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
CIP-002-1	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and	N/A	The Responsible Entity maintained documentation describing its risk-based assessment	The Responsible Entity maintained documentation describing its risk-based assessment	The Responsible Entity did not maintain documentation describing its risk-based assessment

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		evaluation criteria.		methodology which includes evaluation criteria, but does not include procedures.	methodology that includes procedures but does not include evaluation criteria.	methodology that includes procedures and evaluation criteria.
CIP-002-1	R1.2	The risk-based assessment shall consider the following assets:	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.
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.	N/A	N/A	N/A	N/A
CIP-002-1	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-1	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
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.	N/A	N/A	N/A	N/A
CIP-002-1	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		300 MW or more.				
CIP-002-1	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
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.	N/A	N/A	N/A	N/A
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.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-1	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible 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	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-1	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-1	R3.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						criteria in this requirement but was not included in the Critical Cyber Asset List.
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.)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
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:	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security policy.
CIP-003-1	R1.1.	The cyber security policy addresses the requirements	N/A	N/A	N/A	The Responsible Entity's cyber security policy

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		in Standards CIP-002 through CIP-009, including provision for emergency situations.				does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
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.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-1	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
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.	N/A	N/A	N/A	The Responsible Entity has not assigned a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-1	R2.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	N/A	N/A	The senior manager is identified by name, title, and date of designation but the designation is	Identification of the senior manager is missing one of the following: name, title, or date of designation.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					missing business phone or business address.	
CIP-003-1	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
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.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exception from the requirements of the cyber security policy as required.
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).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, 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, in R1, exceptions were not documented.
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).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).
CIP-003-1	R3.2.	Documented exceptions to	N/A	N/A	N/A	The Responsible Entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.				has a documented exception to the cyber security policy 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.
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.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved 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-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.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-1	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum	N/A	N/A	The information protection program does not include one	The information protection program does not include two or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.			of the minimum information types to be protected as detailed in R4.1.	more of the minimum information types to be protected as detailed in R4.1.
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.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
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.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-1	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.
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.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
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.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, 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.
CIP-003-1	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-1	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.				information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
CIP-003-1	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
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.	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-004-1	R1.	Awareness — The Responsible Entity shall	The Responsible Entity established	The Responsible Entity established	The Responsible Entity did document	The Responsible Entity did not establish,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.).	and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. AND The Responsible Entity did not provide security awareness reinforcement on at least a quarterly basis.	but did not establish nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
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.	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to Critical Cyber Assets.	access to Critical Cyber Assets AND The Responsible Entity did not review the training program on an annual basis.	access to Critical Cyber Assets.	
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.	N/A	N/A	N/A	Not all personnel having access to Critical Cyber Assets, including contractors and service vendors, were trained within ninety calendar days of such authorization.
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:	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-1	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-1	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-1	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-1	R2.2.4.	Action plans and procedures to recover or re-establish	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Critical Cyber Assets and access thereto following a Cyber Security Incident.				
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.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
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:	N/A	The Responsible Entity has a personnel risk assessment program, 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, 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.
CIP-004-1	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g.,	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.			Social Security Number verification in the U.S.) or a seven-year criminal check.	Security Number verification in the U.S.) and seven-year criminal check.
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.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
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.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.	The Responsible Entity did not maintain complete 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, missing at least one individual but less than 5% of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 10% or more but less than 15%of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 15% or more of the authorized personnel.
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.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-1	R4.2.	The Responsible Entity shall	N/A	The Responsible	The Responsible	The Responsible Entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.		Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.
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).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
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).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
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).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
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.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-1	R1.5.	Cyber Assets used in the access control and	N/A	N/A	N/A	A Cyber Asset used in the access control and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				monitoring of the Electronic Security Perimeter(s) is not provided 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-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.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of 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.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
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).	N/A	N/A	N/A	The Responsible Entity did not implement or 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-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.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
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.	N/A	N/A	N/A	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, or did not document, individually or by specified grouping, the configuration of those ports and services.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-1	R2.3.	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
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.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-1	R2.5.	The required documentation shall, at least, identify and describe:	N/A	N/A	N/A	The required documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-1	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-1	R2.5.2.	The authentication methods.	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.	N/A	N/A	N/A	N/A
CIP-005-1	R2.5.4.	The controls used to secure	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		dial-up accessible connections.				
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.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
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.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-1	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.				not document electronic or manual processes for monitoring at one or more access points to dial-up devices.
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.	N/A	N/A	N/A	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-005-1	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for one or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:				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 R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-1	R4.1.	A document identifying the vulnerability assessment process;	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;	N/A	N/A	N/A	N/A
CIP-005-1	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	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,	N/A	N/A	N/A	N/A
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.	N/A	N/A	N/A	N/A
CIP-005-1	R5.	Documentation Review and Maintenance — The Responsible Entity shall	The Responsible Entity did not review, update, and	The Responsible Entity did not review, update, and	The Responsible Entity did not review, update, and	The Responsible Entity did not review, update, and maintain greater

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
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.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
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.	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
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.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
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:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created but did not maintain a physical security plan.	The Responsible Entity did not create and maintain a physical security plan.
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.	N/A	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to the Critical Cyber Assets.	Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to the Critical Cyber Assets.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical access to the Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but not processes to identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security plan includes processes to identify all access points through each Physical Security Perimeter but not measures to control entry at those access points.	The Responsible Entity's physical security plan does not include processes to identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
CIP-006-1	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
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.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for the appropriate use of physical access controls as described in Requirement R3.
CIP-006-1	R1.5	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests or does not include revocation of access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						authorization, in accordance with CIP-004 Requirement R4.
CIP-006-1	R1.6	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for escorted access within the physical security perimeter.
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.	N/A	N/A	N/A	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.
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,	N/A	N/A	N/A	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is not afforded one (1) or more of the protective measures specified in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.				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-006-1	R1.9	Process for ensuring that the physical security plan is reviewed at least annually.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include a process for ensuring that the physical security plan is reviewed at least annually.
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:	N/A	N/A	N/A	The Responsible Entity has not documented, or has 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.
CIP-006-1	R2.1.	Card Key: A means of electronic access where the access rights of the card	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		holder are predefined in a computer database. Access rights may differ from one perimeter to another.				
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.	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.	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.	N/A	N/A	N/A	N/A
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	N/A	N/A	N/A	The Responsible Entity **has not documented or has not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the monitoring methods identified in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:				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-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.	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.	N/A	N/A	N/A	N/A
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	N/A	N/A	N/A	The Responsible Entity **has not implemented or has 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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:				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-006-1	R4.1.	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	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.	N/A	N/A	N/A	N/A
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.	N/A	N/A	N/A	N/A
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	The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained physical access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained physical access logs for less than 45 calendar days.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		CIP-008.				
CIP-006-1	R6	Maintenance and Testing — The Responsible Entity shall implement a 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:	N/A	N/A	N/A	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-006-1	R6.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	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.	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.	N/A	N/A	N/A	N/A
CIP-007-1	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant	N/A	N/A	N/A	The Responsible Entity did not ensure the prevention of adverse affects described in R1,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				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-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.	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.	N/A	N/A	N/A	N/A
CIP-007-1	R1.3.	The Responsible Entity shall document test results.	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	N/A	N/A	N/A	The Responsible Entity did not establish or did not document a process to ensure that only those ports and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		required for normal and emergency operations are enabled.				services required for normal and emergency operations are enabled.
CIP-007-1	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).
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).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
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.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure or state an acceptance of risk.
CIP-007-1	R3.	Security Patch Management — The Responsible Entity, either separately or as a	N/A	N/A	N/A	The Responsible Entity **did not establish or did not** document, either

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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).				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-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.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
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	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		mitigate risk exposure or an acceptance of risk.				patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
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).	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more 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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.
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.	N/A	N/A	N/A	The Responsible Entity **did not document or did not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
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	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
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.	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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.	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
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.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
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.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
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	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		other generic account privileges including factory default accounts.				administrator, shared, and other generic account privileges including factory default accounts.
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.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-1	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
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	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		assignment or termination).				the account in the event of personnel changes (for example, change in assignment or termination).
CIP-007-1	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-1	R5.3.1.	Each password shall be a minimum of six characters.	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.	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.	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.	N/A	N/A	N/A	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 on one or more of Cyber Assets inside the Electronic Security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Perimeter(s).
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.	N/A	N/A	N/A	The Responsible Entity **did not implement or 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.
CIP-007-1	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
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.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
CIP-007-1	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-1	R6.5.	The Responsible Entity shall	N/A	N/A	N/A	The Responsible Entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		review logs of system events related to cyber security and maintain records documenting review of logs.				did not review logs of system events related to cyber security nor maintain records documenting review of logs.
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.	N/A	N/A	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 as specified in R7.2.	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						redeployment as specified in R7.3.
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.	N/A	N/A	N/A	N/A
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.	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.	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						8.1, 8.2, 8.3, 8.4.
CIP-007-1	R8.1.	A document identifying the vulnerability assessment process;	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;	N/A	N/A	N/A	N/A
CIP-007-1	R8.3.	A review of controls for default accounts; and,	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.	N/A	N/A	N/A	N/A
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.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually or the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually nor were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
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:	N/A	N/A	The Responsible Entity has developed a Cyber Security Incident response plan that 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.	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.
CIP-008-1	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	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.	N/A	N/A	N/A	N/A
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.	N/A	N/A	N/A	N/A
CIP-008-1	R1.4.	Process for updating the Cyber Security Incident response plan within ninety	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		calendar days of any changes.				
CIP-008-1	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	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.	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.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.
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:	N/A	N/A	N/A	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 address one or more of the requirements CIP- 009-1 R1.1 **and** R1.2.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
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).	N/A	N/A	N/A	N/A
CIP-009-1	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
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.	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						personnel responsible for the activation and implementation of the recovery plan(s) within 90 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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
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.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-001-1	R1	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	MEDIUM
CIP-001-1	R2	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	MEDIUM
CIP-001-1	R3	The risk-based assessment shall consider the following assets:	MEDIUM
CIP-001-1	R4	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	MEDIUM
CIP-002-1	R1.	Transmission substations that support the reliable operation of the Bulk Electric System.	MEDIUM
CIP-002-1	R1.1	Generation resources that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	MEDIUM
CIP-002-1	R1.2.1.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	LOWER
CIP-002-1	R1.2.2.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.3.	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	R1.2.4.	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	R1.2.5.	Critical Cyber Asset Identification — Using the list of Critical	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		Assets developed pursuant to Requirement R2, the Responsible 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	R1.2.6.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	LOWER
CIP-002-1	R1.2.7.	The Cyber Asset uses a routable protocol within a control center; or,	LOWER
CIP-002-1	R2.	The Cyber Asset is dial-up accessible.	HIGH
CIP-002-1	R3.	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.)	HIGH
CIP-002-1	R3.1	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-002-1	R3.2.	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.	LOWER
CIP-002-1	R3.3.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		Assets.	
CIP-002-1	R4.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-1	R1.	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.	MEDIUM
CIP-003-1	R1.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	LOWER
CIP-003-1	R1.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-1	R1.3	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-1	R2.	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).	MEDIUM
CIP-003-1	R2.1.	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	R2.2.	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	R2.3.	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	R3.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-1	R3.1.	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.	LOWER
CIP-003-1	R3.2.	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	R3.3.	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	R4.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	MEDIUM
CIP-003-1	R4.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	MEDIUM
CIP-003-1	R4.2.	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	LOWER
CIP-003-1	R4.3.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-1	R5.	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	R5.1.	The Responsible Entity shall assess and document at least	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		annually the processes for controlling access privileges to protected information.	
CIP-003-1	R5.1.1.	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.	LOWER
CIP-003-1	R5.1.2.	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-003-1	R5.2.	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-003-1	R5.3.	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

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-1	R6.	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	R1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-1	R2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-1	R2.1.	The proper handling of Critical Cyber Asset information; and,	MEDIUM
CIP-004-1	R2.2.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-1	R2.2.1.	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	R2.2.2.	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	R2.2.3.	The Responsible Entity shall ensure that each assessment 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.	LOWER
CIP-004-1	R2.2.4.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		personnel risk assessment or for cause.	
CIP-004-1	R2.3.	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	R3.	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.	MEDIUM
CIP-004-1	R3.1.	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	R3.2.	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
CIP-004-1	R3.3.	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).	LOWER
CIP-004-1	R4.	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-004-1	R4.1.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		Electronic Security Perimeter for that single access point at the dial-up device.	
CIP-004-1	R4.2.	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
CIP-005-1	R1.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	MEDIUM
CIP-005-1	R1.1.	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.	MEDIUM
CIP-005-1	R1.2.	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.	MEDIUM
CIP-005-1	R1.3.	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).	MEDIUM
CIP-005-1	R1.4.	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	R1.5.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		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.	
CIP-005-1	R1.6.	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	LOWER
CIP-005-1	R2.	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.	MEDIUM
CIP-005-1	R2.1.	The required documentation shall, at least, identify and describe:	MEDIUM
CIP-005-1	R2.2.	The processes for access request and authorization.	MEDIUM
CIP-005-1	R2.3.	The authentication methods.	MEDIUM
CIP-005-1	R2.4.	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.	MEDIUM
CIP-005-1	R2.5.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-1	R2.5.1.	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
CIP-005-1	R2.5.2.	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	R2.5.3.	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	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		to the dial-up device, where technically feasible.	
CIP-005-1	R2.5.4.	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	R2.6.	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	R3.	A document identifying the vulnerability assessment process;	MEDIUM
CIP-005-1	R3.1.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-1	R3.2.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-1	R4.	A review of controls for default accounts, passwords, and network management community strings; and,	MEDIUM
CIP-005-1	R4.1.	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	R4.2.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	MEDIUM
CIP-005-1	R4.3.	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.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-1	R4.4.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	MEDIUM
CIP-005-1	R4.5.	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.	MEDIUM
CIP-005-1	R5.	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:	LOWER
CIP-005-1	R5.1.	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.	LOWER
CIP-005-1	R5.2.	Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.	LOWER
CIP-005-1	R5.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	LOWER
CIP-006-1	R1.	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	R1.1.	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	MEDIUM
CIP-006-1	R1.2.	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		access.	
CIP-006-1	R1.3	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.	MEDIUM
CIP-006-1	R1.4	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.	MEDIUM
CIP-006-1	R1.5	Process for ensuring that the physical security plan is reviewed at least annually.	MEDIUM
CIP-006-1	R1.6	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	R1.7	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.	LOWER
CIP-006-1	R1.8	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.	LOWER
CIP-006-1	R1.9	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	LOWER
CIP-006-1	R2	Other Authentication Devices: Biometric, keypad, token, or	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		other equivalent devices that control physical access to the Critical Cyber Assets.	
CIP-006-1	R2.1.	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	R2.2.	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	R2.3.	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.	MEDIUM
CIP-006-1	R2.4.	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:	MEDIUM
CIP-006-1	R3	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	MEDIUM
CIP-006-1	R3.1.	Video Recording: Electronic capture of video images of sufficient quality to determine identity.	MEDIUM
CIP-006-1	R3.2.	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

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-1	R4	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	R4.1.	Maintenance and Testing — The Responsible Entity shall implement a 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:	LOWER
CIP-006-1	R4.2.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	LOWER
CIP-006-1	R4.3.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	LOWER
CIP-006-1	R5	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-006-1	R6	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-006-1	R6.1.	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.	MEDIUM
CIP-006-1	R6.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-006-1	R6.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-1	R1.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		services required for normal and emergency operations are enabled.	
CIP-007-1	R1.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	LOWER
CIP-007-1	R1.2.	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).	LOWER
CIP-007-1	R1.3.	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	R2.	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).	MEDIUM
CIP-007-1	R2.1.	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.	MEDIUM
CIP-007-1	R2.2.	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.	MEDIUM
CIP-007-1	R2.3.	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).	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-1	R3.	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	R3.1.	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	R3.2.	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	R4.	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.	MEDIUM
CIP-007-1	R4.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	MEDIUM
CIP-007-1	R4.2.	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.	MEDIUM
CIP-007-1	R5.	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	R5.1.	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	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		factory default accounts.	
CIP-007-1	R5.1.1.	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	R5.1.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-1	R5.1.3.	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).	MEDIUM
CIP-007-1	R5.2.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-1	R5.2.1.	Each password shall be a minimum of six characters.	MEDIUM
CIP-007-1	R5.2.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-1	R5.2.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-1	R5.3.	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	R5.3.1.	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	R5.3.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	LOWER
CIP-007-1	R5.3.3.	The Responsible Entity shall maintain logs of system events	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.	
CIP-007-1	R6.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-1	R6.1.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	MEDIUM
CIP-007-1	R6.2.	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.	MEDIUM
CIP-007-1	R6.3.	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.	MEDIUM
CIP-007-1	R6.4.	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	R6.5.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-1	R7.	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	R7.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-1	R7.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-1	R7.3.	A review of controls for default accounts; and,	LOWER
CIP-007-1	R8	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-007-1	R8.1.	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
CIP-007-1	R8.2.	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:	MEDIUM
CIP-007-1	R8.3.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	MEDIUM
CIP-007-1	R8.4.	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	MEDIUM
CIP-007-1	R9	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.	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	LOWER
CIP-008-1	R1.1.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-1	R1.2.	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	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		operational exercise, to the response to an actual incident.	
CIP-008-1	R1.3.	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
CIP-008-1	R1.4.	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:	LOWER
CIP-008-1	R1.5.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	LOWER
CIP-008-1	R1.6.	Define the roles and responsibilities of responders.	LOWER
CIP-008-1	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	R1	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.	MEDIUM
CIP-009-1	R1.1.	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.	MEDIUM
CIP-009-1	R1.2.	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.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-009-1	R2		LOWER
CIP-009-1	R3		LOWER
CIP-009-1	R4		LOWER
CIP-009-1	R5		LOWER

EXHIBIT B

CIP VIOLATION RISK FACTORS AND VIOLATION SEVERITY LEVELS – VERSION 2
(CLEAN AND REDLINE)

CIP Version 2 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-2	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
CIP-002-2	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
CIP-002-2	R1.2	The risk-based assessment shall consider the following assets:	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.
CIP-002-2	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	N/A	N/A	N/A	N/A
CIP-002-2	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-2	R1.2.3.	Generation resources that support	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the reliable operation of the Bulk Electric System.				
CIP-002-2	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.	N/A	N/A	N/A	N/A
CIP-002-2	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	N/A	N/A	N/A	N/A
CIP-002-2	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-2	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.	N/A	N/A	N/A	N/A
CIP-002-2	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.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-2	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:			but the list has not been reviewed and updated annually as required.	per requirement R2 even if such list is null.
CIP-002-2	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-2	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-2	R3.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	A Cyber Asset essential to the operation of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-2	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, 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 risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets **or** the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-2	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:	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security policy.
CIP-003-2	R1.1.	The cyber security policy addresses	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.				Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-2	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-2	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Standards CIP-002 through CIP-009.
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
CIP-003-2	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					calendar days of the effective date.	are not documented within thirty calendar days of the effective date.
CIP-003-2	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-2	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).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, 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, in R1, exceptions were not documented.
CIP-003-2	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).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).
CIP-003-2	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception	N/A	N/A	The Responsible Entity has a documented	The Responsible Entity has a documented

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		is necessary and any compensating measures.			exception to the cyber security policy in R1 but did not include **either**: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	exception to the cyber security policy in R1 but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-2	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.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved 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-003-2	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-2	R4.1.	The Critical Cyber Asset information	N/A	N/A	The information	The information

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, 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.			protection program does not include one of the minimum information types to be protected as detailed in R4.1.	protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.
CIP-003-2	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-2	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.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible Entity did not implement an action plan to remediate

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						deficiencies identified during the assessment.
CIP-003-2	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.
CIP-003-2	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-2	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, 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.
CIP-003-2	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		annually.				list of personnel responsible for authorizing access to protected information.
CIP-003-2	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.	N/A	N/A	N/A	The Responsible Entity did not 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.
CIP-003-2	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-2	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	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control process for the activities required in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-004-2	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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,	N/A	N/A	The Responsible[[1]] Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		etc.).				
CIP-004-2	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	N/A	N/A	The Responsible[2] Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, or document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-2	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A	N/A	N/A	Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-2	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1,

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		required items appropriate to personnel roles and responsibilities:				R2.2.2, R2.2.3, R2.2.4.
CIP-004-2	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-2	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-2	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-2	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-2	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.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
CIP-004-2	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to	N/A	The Responsible Entity has a personnel risk assessment program, , 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 after such personnel were granted such access except in specified	The Responsible Entity does not have a documented personnel risk assessment program, as stated in R3, for personnel having authorized cyber or authorized unescorted physical access.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:			circumstances such as an emergency.	OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
CIP-004-2	R3.1.	The Responsible Entity shall ensure that each assessment 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.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-2	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.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				when applicable.	personnel risk assessment.	when applicable.
CIP-004-2	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-004-2.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-2	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.	The Responsible Entity did not maintain complete 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, missing at least one individual but less than 5% of the authorized	The Responsible Entity did not maintain complete 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, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 10% or more but less than 15%of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 15% or more of the authorized personnel.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			personnel.			
CIP-004-2	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.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-2	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.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.
CIP-005-2	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	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Electronic Security Perimeter(s) and all access points to the perimeter(s).				Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-2	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).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-2	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.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
CIP-005-2	R1.3.	Communication links connecting	N/A	N/A	N/A	At least one end

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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).				point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-2	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-005-2.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-2	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	N/A	N/A	N/A	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded one (1) or more of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3;

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement~~s~~ R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.
CIP-005-2	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.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of 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-005-2	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).				implement or 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-005-2	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.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-2	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.	N/A	N/A	N/A	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, or did not document,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						individually or by specified grouping, the configuration of those ports and services.
CIP-005-2	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not implement or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-2	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.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-2	R2.5.	The required documentation shall, at least, identify and describe:	N/A	N/A	N/A	The required documentation for R2 did not include one or more of the elements described in R2.5.1 through

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R2.5.4.
CIP-005-2	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-2	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-2	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-2	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-2	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.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
CIP-005-2	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	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		day, seven days a week.				logging access points.
CIP-005-2	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.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at one or more access points to dial-up devices.
CIP-005-2	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.	N/A	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
CIP-005-2	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 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 R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-2	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-2	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-2	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-2	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-2	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.	N/A	N/A	N/A	N/A
CIP-005-2	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
CIP-005-2	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP- 005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
CIP-005-2	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.	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar days of the change.
CIP-005-2	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-008-2.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security plan.	The Responsible Entity did not document, implement, and maintain a physical security plan.
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed or documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter or does not identify measures to control entry at those access points.
CIP-006-2	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						monitor physical access to the perimeter(s).
CIP-006-2	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-2	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the review of access authorization requests or the revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
CIP-006-2	R1.6	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.
CIP-006-2	R1.7	Update of the physical security plan within thirty calendar days of the	N/A	N/A	N/A	The Responsible Entity's physical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.				security plan does not address updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.
CIP-006-2	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-2	R2	Protection of Physical Access Control	N/A	N/A	N/A	A Cyber Asset that

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:				authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was not afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3;

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
CIP-006-2	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	N/A	N/A	N/A	N/A
CIP-006-2	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) does not reside within an identified Physical Security Perimeter.
CIP-006-2	R4	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	N/A	N/A	N/A	The Responsible Entity has not documented or has not implemented the operational and procedural controls to manage physical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets				access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-2	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by	N/A	N/A	N/A	The Responsible Entity **has not documented or has not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		authorized personnel as specified in Requirement R4.				immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-2.
CIP-006-2	R6	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:	N/AT	N/A	N/A	The Responsible Entity **has not implemented or has 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4				following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						individuals and the time of access twenty-four hours a day, seven days a week.
CIP-006-2	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.	N/A	N/A	N/A	The responsible entity did not retain physical access logs for at least ninety calendar days.
CIP-006-2	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-2	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-2	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-2	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-007-2	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-007-2, 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.	N/A	N/A	N/A	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-007-2	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.	N/A	N/A	N/A	N/A
CIP-007-2	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-2	R1.3.	The Responsible Entity shall	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		document test results.				
CIP-007-2	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A	N/A	The Responsible Entity did not establish (implement) or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
CIP-007-2	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-2	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).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-2	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.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk.
CIP-007-2	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement 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).	N/A	N/A	N/A	The Responsible Entity **did not establish (implement) or did not document**, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk.
CIP-007-2	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	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).				other malicious software ("malware") prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-2	R4.2.	The Responsible Entity shall document and implement a process for the update of	N/A	N/A	N/A	The Responsible Entity **did not document or did**

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.				**not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention “signatures.”
CIP-007-2	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	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not 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-007-2	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirement R5.				implemented as approved by designated personnel.
CIP-007-2	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.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-2	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						privileges including factory default accounts.
CIP-007-2	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.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-2	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-2	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).	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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-007-2	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-2	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-2	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-2	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-2	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	N/A	N/A	N/A	The Responsible Entity as technically feasible, did not implement automated tools or organizational process controls, to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		related to cyber security.				monitor system events that are related to cyber security on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity **did not implement or 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.
CIP-007-2	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-2	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-008-2.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						technically feasible, to support incident response as required in Standard CIP-008.
CIP-007-2	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-2	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-2	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.	N/A	N/A	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 **but** did not address redeployment as	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					specified in R7.2.	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-005-2 but did not address disposal as specified in R7.1. OR The Responsible Entity did not maintain records pertaining to disposal or redeployment as specified in R7.3.[[3]]
CIP-007-2	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to	N/A	N/A	N/A	N/A

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		prevent unauthorized retrieval of sensitive cyber security or reliability data.				
CIP-007-2	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.	N/A	N/A	N/A	N/A
CIP-007-2	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-2	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment 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-007-2	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-2	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Electronic Security Perimeter are enabled;				
CIP-007-2	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-2	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.	N/A	N/A	N/A	N/A
CIP-007-2	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually **and** changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being completed.
CIP-008-2	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber	N/A	N/A	The Responsible Entity has developed a Cyber Security Incident response plan that addresses all of the	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Security Incident response plan shall address, at a minimum, the following:			components required by R1.1 through R1.6 but has not maintained the plan in accordance with those components.	components required by R1.1 through R1.6, or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-2	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-2	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-2	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.	N/A	N/A	N/A	N/A
CIP-008-2	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	N/A	N/A	N/A	N/A
CIP-008-2	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-2	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.				
CIP-008-2	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.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-009-2	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:	N/A	N/A	N/A	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 address one or more of the requirements CIP-009-1 R1.1 **and** R1.2.
CIP-009-2	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-2	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-009-2	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-2	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 thirty calendar days of the change being completed.	N/A	N/A	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)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						within thirty calendar days of the change.
CIP-009-2	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-2	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.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

VRFs

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-2	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	MEDIUM
CIP-002-2	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-2	R1.2	The risk-based assessment shall consider the following assets:	MEDIUM
CIP-002-2	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-002-2	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-2	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-2	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-002-2	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-002-2	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-2	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-002-2	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.	HIGH
CIP-002-2	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible 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-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	HIGH
CIP-002-2	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	LOWER
CIP-002-2	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	LOWER
CIP-002-2	R3.3.	The Cyber Asset is dial-up accessible.	LOWER
CIP-002-2	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, 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 risk-	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	
CIP-003-2	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:	MEDIUM
CIP-003-2	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.	LOWER
CIP-003-2	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-003-2	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.	MEDIUM
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-2	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).	LOWER
CIP-003-2	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-003-2	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOWER
CIP-003-2	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

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-2	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-2	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-002-2, 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.	MEDIUM
CIP-003-2	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-003-2	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-003-2	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-2	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-003-2	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	LOWER
CIP-003-2	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-2	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-003-2	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-2	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.	LOWER
CIP-004-2	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		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.).	
CIP-004-2	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOWER
CIP-004-2	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MEDIUM
CIP-004-2	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-2	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-2	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-2	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-2	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-2	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-004-2	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	MEDIUM
CIP-004-2	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and sevenyear 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.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-004-2	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-004-2	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-004-2.	LOWER
CIP-004-2	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-004-2	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-004-2	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
CIP-005-2	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-005-2	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).	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	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).	MEDIUM
CIP-005-2	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-005-2.	MEDIUM
CIP-005-2	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	
CIP-005-2	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-005-2	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).	MEDIUM
CIP-005-2	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-005-2	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-005-2	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-2	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-2	R2.5.2.	The authentication methods.	LOWER
CIP-005-2	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.	LOWER
CIP-005-2	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-2	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
CIP-005-2	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.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-2	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.	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	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:	MEDIUM
CIP-005-2	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-2	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-2	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-2	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.	LOWER
CIP-005-2	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.	LOWER
CIP-005-2	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-005-2	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-008-2.	LOWER
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8	Annual review of the physical security plan.	LOWER
CIP-006-2	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM
CIP-006-2	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM
CIP-006-2	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-2	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets	MEDIUM
CIP-006-2	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-2	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		determine identity. - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	
CIP-006-2	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.	LOWER
CIP-006-2	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-2	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-2	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-2	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-2	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-007-2, 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-007-2	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-007-2	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-2	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-2	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MEDIUM
CIP-007-2	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-2	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-007-2	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.	MEDIUM
CIP-007-2	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement 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-007-2	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-007-2	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.	LOWER
CIP-007-2	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).	MEDIUM
CIP-007-2	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.	MEDIUM
CIP-007-2	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.	MEDIUM
CIP-007-2	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-007-2	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.	MEDIUM
CIP-007-2	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-2	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-007-2	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.	MEDIUM
CIP-007-2	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-007-2	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.	MEDIUM
CIP-007-2	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-2	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).	MEDIUM
CIP-007-2	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-2	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-2	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-2	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-2	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-007-2	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.	MEDIUM
CIP-007-2	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-2	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-008-2.	MEDIUM
CIP-007-2	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		calendar days.	
CIP-007-2	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-2	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.	LOWER
CIP-007-2	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-007-2	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-007-2	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-2	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-007-2	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-2	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;	MEDIUM
CIP-007-2	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-2	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.	MEDIUM
CIP-007-2	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOWER
CIP-008-2	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOWER
CIP-008-2	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER
CIP-008-2	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		response teams, Cyber Security Incident handling procedures, and communication plans.	
CIP-008-2	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-008-2	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	LOWER
CIP-008-2	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-2	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.	LOWER
CIP-008-2	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
CIP-009-2	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-009-2	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-009-2	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-2	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-009-2	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 thirty calendar days of the change being completed.	LOWER
CIP-009-2	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-009-2	R5	Testing Backup Media — Information essential to recovery that is stored on backup	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	

CIP Version 2 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-2	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
CIP-002-2	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
CIP-002-2	R1.2	The risk-based assessment shall consider the following assets:	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.
CIP-002-2	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	N/A	N/A	N/A	N/A
CIP-002-2	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-2	R1.2.3.	Generation resources that support	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the reliable operation of the Bulk Electric System.				
CIP-002-2	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.	N/A	N/A	N/A	N/A
CIP-002-2	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	N/A	N/A	N/A	N/A
CIP-002-2	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-2	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.	N/A	N/A	N/A	N/A
CIP-002-2	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.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-2	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:			but the list has not been reviewed and updated annually as required.	per requirement R2 even if such list is null.
CIP-002-2	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-2	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-2	R3.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	A Cyber Asset essential to the operation of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-2	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, 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 risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets **or** the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-2	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:	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security policy.
CIP-003-2	R1.1.	The cyber security policy addresses	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.				Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-2	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-2	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Standards CIP-002 through CIP-009.
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
CIP-003-2	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					calendar days of the effective date.	are not documented within thirty calendar days of the effective date.
CIP-003-2	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-2	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).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, 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, in R1, exceptions were not documented.
CIP-003-2	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).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).
CIP-003-2	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception	N/A	N/A	The Responsible Entity has a documented	The Responsible Entity has a documented

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		is necessary and any compensating measures.			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.	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.
CIP-003-2	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.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved 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-003-2	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information associated with

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Critical Cyber Assets.
CIP-003-2	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-002-2, 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.	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.
CIP-003-2	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-2	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.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-2	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.
CIP-003-2	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-2	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, 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.
CIP-003-2	R5.1.2.	The list of personnel responsible for	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		authorizing access to protected information shall be verified at least annually.				Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-2	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.	N/A	N/A	N/A	The Responsible Entity did not 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.
CIP-003-2	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-2	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-004-2	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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	N/A~~The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~	N/A~~The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~ The Responsible[1] Entity did not	The Responsible Entity did not establish, implement, maintain, ~~nor~~ or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reinforcement (e.g., presentations, meetings, etc.).			provide security awareness reinforcement on at least a quarterly basis.	
CIP-004-2	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	N/A~~The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~	N/A~~The Responsibility Entity did not review the training program on an annual basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~ The Responsible[2] Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, ~~nor~~or document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-2	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A~~At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained~~	N/A~~At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being~~	N/A~~At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being~~	~~15% or more of~~ Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were ~~not~~ trained prior to their being granted such access

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~prior to their being granted such access except in specified circumstances such as an emergency.~~	~~granted such access except in specified circumstances such as an emergency.~~	~~granted such access except in specified circumstances such as an emergency.~~	except in specified circumstances such as an emergency.
CIP-004-2	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-2	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-2	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-2	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-2	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-2	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.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
CIP-004-2	R3.	Personnel Risk Assessment —The Responsible Entity shall have a	N/A	The Responsible Entity has a	The Responsible Entity has a	The Responsible Entity does not have

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:		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.	personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	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 except in specified circumstances such as an emergency.
CIP-004-2	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included	The Responsible Entity did not ensure that each assessment

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.			an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-2	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.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-2	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-004-2.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-004-2	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.	The Responsible Entity did not maintain complete 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, missing at least one individual but less than 5% of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 10% or more but less than 15%of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 15% or more of the authorized personnel.
CIP-004-2	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.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-2	R4.2.	The Responsible Entity shall revoke	N/A	The Responsible	The Responsible	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.		Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.
CIP-005-2	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).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-2	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).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						device within the Electronic Security Perimeter(s).
CIP-005-2	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.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
CIP-005-2	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).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-2	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-005-2.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-2	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3, Standard CIP-007-2 Requirements R1 and R3 through R9;, Standard CIP-008-2; and Standard CIP-009-2.~~	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3;, Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9;, Standard CIP-008-2; and Standard CIP-009-2.~~	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.~~	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not ~~is not provided~~afforded ~~without four (4)~~ one (1) or more of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement~~s~~ R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.
CIP-005-2	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	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of one or more of the following: Electronic Security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.				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-005-2	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).	N/A	N/A	N/A	The Responsible Entity did not implement or 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-005-2	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.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						default, such that explicit access permissions must be specified.
CIP-005-2	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.	N/A	N/A	N/A	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, or did not document, individually or by specified grouping, the configuration of those ports and services.
CIP-005-2	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A~~The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.~~	The Responsible Entity did not implement or~~nor~~ maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-2	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the	N/A	N/A	N/A	Where external interactive access into the Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.				Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-2	R2.5.	The required documentation shall, at least, identify and describe:	N/A	N/A	N/A	The required documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-2	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-2	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-2	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-2	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-2	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	The Responsible Entity did not maintain a document identifying the content of the banner.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		identifying the content of the banner.	OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	screen upon all interactive access attempts.	screen upon all interactive access attempts.	screen upon all interactive access attempts.
CIP-005-2	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.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-2	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.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at one or more access points to dial-up devices.
CIP-005-2	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	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement security monitoring

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				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-005-2	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for one or more of the access points to the Electronic Security Perimeter(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The vulnerability assessment did not include one (1) or more of the subrequirements R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-2	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-2	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-2	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-2	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-2	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.	N/A	N/A	N/A	N/A
CIP-005-2	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-2	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
CIP-005-2	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.	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-2	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-008-2.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).	The Responsible Entity did not document, implement, and maintain a physical security plan.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity created and implemented but did not maintain a physical security plan.	
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	N/A~~Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	~~Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~N/A	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed or~~and~~ documented alternative measures to control physical~~-~~ access to such Cyber Assets within the Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Perimeter.
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A~~The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.~~	N/A~~The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.~~	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter ~~n~~or does not identify measures to control entry at those access points.
CIP-006-2	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-2	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-2	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	N/A	N/A	N/A~~The Responsible Entity's physical security plan does not address either~~	The Responsible Entity's physical security plan does not address the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.~~	~~process for~~ review~~ing~~ of access authorization requests ~~and~~or the ~~process for~~ revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
CIP-006-2	R1.6	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.
CIP-006-2	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	N/A~~The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration **but** the plan was not updated within thirty calendar days of the completion of a physical security~~	The Responsible Entity's physical security plan does not address ~~a process for~~ updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~system redesign or reconfiguration.~~	OR The plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.
CIP-006-2	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-2	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the~~	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the~~	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of~~	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.~~	~~protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.~~	~~the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.~~	OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was ~~provided without~~ not afforded ~~four (4) or more of~~ the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
CIP-006-2	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	N/A	N/A	N/A	N/A
CIP-006-2	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) does~~did~~ not reside within an identified Physical Security Perimeter.
CIP-006-2	R4	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: - 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.	N/A	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 one or more of the following physical access methods:~~ ~~• Card Key: A~~	N/A~~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 one or more of the following physical access methods:~~ ~~• Card Key: A~~	The Responsible Entity has not documented ~~n~~or has 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 one or more of the following physical access methods: • Card Key: A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets		~~means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.~~	~~means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.~~	means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-2	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	N/A	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) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.~~ ~~• Human Observation of Access Points: Monitoring of physical access points by authorized~~	N/A~~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) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.~~ ~~• Human Observation of Access Points: Monitoring of physical access points by authorized~~	The Responsible Entity **has not documented ~~n~~or** has not **implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~personnel as specified in Requirement R4.~~	~~personnel as specified in Requirement R4.~~	points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-2.
CIP-006-2	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book	N/AT~~he Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~	N/A~~The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording:~~	N/A~~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 following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~	The Responsible Entity **has not implemented** ~~**n**~~**or has not documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, 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.~~	~~Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4,~~ ~~**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.~~	~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.~~	monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.
CIP-006-2	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to	N/A~~The Responsible Entity retained physical access logs for 75 or more~~	N/A~~The Responsible Entity retained physical access logs for 60 or more~~	N/A~~The Responsible Entity retained physical access logs for 45 or more~~	~~The Responsible Entity retained physical access logs for less than 45~~

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.	~~calendar days, but for less than 90 calendar days.~~	~~calendar days, but for less than 75 calendar days.~~	~~calendar days, but for less than 60 calendar days.~~	~~calendar days.~~ The responsible entity did not retain physical access logs for at least ninety calendar days.
CIP-006-2	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include one of the Requirements R8.1, R8.2, and R8.3.~~	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include two of the Requirements R8.1, R8.2, and R8.3.~~	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include any of the Requirements R8.1, R8.2, and R8.3.~~	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-2	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-2	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-2	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		one calendar year.				
CIP-007-2	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-007-2, 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.	N/A	N/A	N/A	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-007-2	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.	N/A	N/A	N/A	N/A
CIP-007-2	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-2	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-2	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A~~The Responsible Entity **established (implemented) but did not document** a process to ensure that only those ports and services~~	N/A~~The Responsible Entity **documented but did not establish (implement)** a process to ensure that only those ports~~	The Responsible Entity did not establish (implement) ~~n~~or did not document a process to ensure that only those ports

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~required for normal and emergency operations are enabled.~~	~~and services required for normal and emergency operations are enabled.~~	and services required for normal and emergency operations are enabled.
CIP-007-2	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-2	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).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-2	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.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						measure(s) applied to mitigate risk. ~~exposure or state an acceptance of risk.~~
CIP-007-2	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement 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).	N/A~~The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-2 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).~~	N/A~~The Responsible Entity~~ ~~**established (implemented) but did not document**~~~~, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	N/A~~The Responsible Entity~~ ~~**documented but did not establish (implement)**~~~~, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	The Responsible Entity **did not establish (implement)** ~~**n**~~**or** did not **document**, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk. ~~exposure or an acceptance of risk.~~
CIP-007-2	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).	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more Cyber

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Assets within the Electronic Security Perimeter(s).
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity **did not document or did not implement** a process including addressing testing and installing the signatures for the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						update of anti-virus and malware prevention “signatures.”
CIP-007-2	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	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not 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-007-2	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-2	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.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-2	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-2	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.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-2	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-2	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).	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						for securing the account in the event of personnel changes (for example, change in assignment or termination).
CIP-007-2	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-2	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-2	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and "special" characters.	N/A	N/A	N/A	N/A
CIP-007-2	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity as technically feasible, did not implement automated tools or organizational process controls, to monitor system events that are related to cyber

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						security on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-2	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.	N/A	N/A	N/A	The Responsible Entity **did not implement or 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.
CIP-007-2	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-2	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-008-2.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						required in Standard CIP-008.
CIP-007-2	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-2	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-2	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.	N/A~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 **but** did not maintain records as specified in R7.3.~~	N/A~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 **but** did not address redeployment as specified in R7.2.~~	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 **but** did not address ~~disposal~~ redeployment as specified in R7.2~~1~~.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2. OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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-005-2 but did not address disposal as specified in R7.1. OR The Responsible Entity did not maintain records pertaining to disposal or redeployment as specified in R7.3.[3]
CIP-007-2	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.	N/A	N/A	N/A	N/A

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-2	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.	N/A	N/A	N/A	N/A
CIP-007-2	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-2	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment 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-007-2	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-2	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;	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-2	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-2	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.	N/A	N/A	N/A	N/A
CIP-007-2	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually ~~nor~~ and ~~were~~ changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being completed.
CIP-008-2	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the	N/A	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 addresses all of the components required by R1.1	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all of the components required by R1.1

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		following:			through R1.6 but has not maintained the plan in accordance with those components. ~~but the plan does not address one or more of the subrequirements R1.1 through R1.6.~~	through R1.6, or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-2	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-2	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-2	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.	N/A	N/A	N/A	N/A
CIP-008-2	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	N/A	N/A	N/A	N/A
CIP-008-2	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-2	R1.6.	Process for ensuring the Cyber Security Incident response plan is	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.				
CIP-008-2	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.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-009-2	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:	N/A	N/A	N/A	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 address one or more of the requirements CIP-009-1 R1.1 **and** R1.2.
CIP-009-2	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-009-2	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-2	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-2	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 thirty calendar days of the change being completed.	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 than30 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.~~	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						implementation of the recovery plan(s) within ~~more than~~ thirty ~~180~~ calendar days of the change.
CIP-009-2	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-2	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.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

VRFs

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-2	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-2	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	LOWER
CIP-002-2	R1.2	The risk-based assessment shall consider the following assets:	MEDIUM
CIP-002-2	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-002-2	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-2	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-2	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-002-2	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-002-2	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-2	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-002-2	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.	HIGH
CIP-002-2	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible 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-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	HIGH
CIP-002-2	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	LOWER
CIP-002-2	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	LOWER
CIP-002-2	R3.3.	The Cyber Asset is dial-up accessible.	LOWER
CIP-002-2	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		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 risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	
CIP-003-2	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:	MEDIUM
CIP-003-2	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.	LOWER
CIP-003-2	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-003-2	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.	MEDIUM~~LOWER~~
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-2	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-2	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-2	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-2	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).	LOWER
CIP-003-2	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-003-2	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-2	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-003-2	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-2	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-002-2, 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.	MEDIUM
CIP-003-2	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-003-2	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-003-2	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-2	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-003-2	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	LOWER
CIP-003-2	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-2	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-003-2	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-2	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.	LOWER
CIP-004-2	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		authorized unescorted physical access to Critical Cyber Assets 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.).	
CIP-004-2	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOWER
CIP-004-2	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MEDIUM
CIP-004-2	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-2	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-2	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-2	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-2	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-2	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-004-2	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	MEDIUM
CIP-004-2	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and sevenyear	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		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-004-2	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-004-2	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-004-2.	LOWER
CIP-004-2	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-004-2	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-004-2	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
CIP-005-2	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-005-2	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).	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	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).	MEDIUM
CIP-005-2	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-005-2.	MEDIUM
CIP-005-2	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	
CIP-005-2	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-005-2	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).	MEDIUM
CIP-005-2	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-005-2	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-005-2	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-2	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-2	R2.5.2.	The authentication methods.	LOWER
CIP-005-2	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.	LOWER
CIP-005-2	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-2	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

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-2	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.	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	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:	MEDIUM
CIP-005-2	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-2	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-2	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-2	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	MEDIUM
CIP-005-2	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.	MEDIUM
CIP-005-2	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.	LOWER
CIP-005-2	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.	LOWER
CIP-005-2	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-005-2	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-008-2.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-2	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-2	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-2	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-2	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MEDIUM
CIP-006-2	R1.6	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-2	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-2	R1.8	Annual review of the physical security plan.	LOWER
CIP-006-2	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM
CIP-006-2	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-2	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-2	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets	MEDIUM
CIP-006-2	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-2	R6	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

Standard Number	Requirement Number	Text of Requirement	VRF
		- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. - Video Recording: Electronic capture of video images of sufficient quality to determine identity. - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	
CIP-006-2	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.	LOWER
CIP-006-2	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-2	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-2	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-2	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-2	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-007-2, 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-007-2	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-007-2	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-2	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-2	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		operations are enabled.	
CIP-007-2	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MEDIUM
CIP-007-2	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-007-2	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.	MEDIUM
CIP-007-2	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement 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-007-2	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-007-2	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.	LOWER
CIP-007-2	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).	MEDIUM
CIP-007-2	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.	MEDIUM
CIP-007-2	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.	MEDIUM
CIP-007-2	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-007-2	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	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		respect to work functions performed.	
CIP-007-2	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.	LOWER
CIP-007-2	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-007-2	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.	MEDIUM
CIP-007-2	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-007-2	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.	MEDIUM
CIP-007-2	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-2	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).	MEDIUM
CIP-007-2	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-2	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-2	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-2	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-2	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-007-2	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.	MEDIUM
CIP-007-2	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-2	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security,	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		where technically feasible, to support incident response as required in Standard CIP-008-2.	
CIP-007-2	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-2	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-2	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.	LOWER
CIP-007-2	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-007-2	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-007-2	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-2	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-007-2	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-2	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;	MEDIUM
CIP-007-2	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-2	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.	MEDIUM
CIP-007-2	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOWER
CIP-008-2	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-008-2	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER
CIP-008-2	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	LOWER
CIP-008-2	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-008-2	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	LOWER
CIP-008-2	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-2	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.	LOWER
CIP-008-2	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
CIP-009-2	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-009-2	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-009-2	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-2	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-009-2	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 thirty calendar days of the change being completed.	LOWER
CIP-009-2	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,	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		written documentation of configuration settings, tape backup, etc.	
CIP-009-2	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

EXHIBIT C

CIP VIOLATION RISK FACTORS AND VIOLATION SEVERITY LEVELS – VERSION 3
(CLEAN AND REDLINE)

CIP Version 3 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-3	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
CIP-002-3	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
CIP-002-3	R1.2	The risk-based assessment shall consider the following assets:	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.
CIP-002-3	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-3	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	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.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	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.	N/A	N/A	N/A	N/A
CIP-002-3	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.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-3	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:			Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	operation of the Critical Asset list as per requirement R2 even if such list is null.
CIP-002-3	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R3.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	A Cyber Asset

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, 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 risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets **or** the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-3	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,	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security policy.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		at minimum, ensure the following:				
CIP-003-3	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-3	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-3	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-3	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-002-3 through CIP-009-3.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-3	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-3	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
CIP-003-3	R2.3.	Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					delegated authority are not documented within thirty calendar days of the effective date.	changes to the delegated authority are not documented within thirty calendar days of the effective date.
CIP-003-3	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-3	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).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, 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, in R1, exceptions were not documented.
CIP-003-3	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).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-3	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not include **either**: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-3	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.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved 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-003-3	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						associated with Critical Cyber Assets.
CIP-003-3	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-002-3, 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.	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.
CIP-003-3	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-3	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.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Entity did not implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-3	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.
CIP-003-3	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-3	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, 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.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-3	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-3	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.	N/A	N/A	N/A	The Responsible Entity did not 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.
CIP-003-3	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-3	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and	N/A	N/A	N/A	The Responsible Entity has not established or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-004-3	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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,	N/A	N/A	The Responsible[[1]] Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		brochures, etc.); - Management support and reinforcement (e.g., presentations, meetings, etc.).				
CIP-004-3	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	N/A	N/A	The Responsible[[2]] Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, or document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-3	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A	N/A	N/A	Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were trained prior to their being granted such access except in specified circumstances such as an emergency.

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-004-3	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-3	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-3	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.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
CIP-004-3	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	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R3, for personnel having authorized	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk	The Responsible Entity does not have a documented personnel risk assessment program, as stated in R3, for personnel

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:		cyber or authorized unescorted physical access, but the program is not documented.	assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	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 except in specified circumstances such as an emergency.
CIP-004-3	R3.1.	The Responsible Entity shall ensure that each assessment 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.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-3	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.	N/A	The Responsible Entity did not update each personnel risk assessment at least	The Responsible Entity did not update each personnel risk assessment for	The Responsible Entity did not update each personnel risk assessment at least

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				every seven years after the initial personnel risk assessment but did update it for cause when applicable.	cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-3	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-004-3.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-3	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.	The Responsible Entity did not maintain complete 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	The Responsible Entity did not maintain complete 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	The Responsible Entity did not maintain complete 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	The Responsible Entity did not maintain complete 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	Cyber Assets, missing 10% or more but less than 15%of the authorized personnel.	Cyber Assets, missing 15% or more of the authorized personnel.
CIP-004-3	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.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-3	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.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-3	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).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-3	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).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-3	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.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Perimeter for that single access point at the dial-up device.
CIP-005-3	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).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-3	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-005-3.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-3	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3	N/A	N/A	N/A	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded one (1) or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.				more of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3c Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.
CIP-005-3	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.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						access control and monitoring of these access points.
CIP-005-3	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).	N/A	N/A	N/A	The Responsible Entity did not implement or 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-005-3	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.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-3	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,	N/A	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the configuration of those ports and services.				monitoring Cyber Assets within the Electronic Security Perimeter, or did not document, individually or by specified grouping, the configuration of those ports and services.
CIP-005-3	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not implement or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-3	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.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-3	R2.5.	The required documentation shall, at	N/A	N/A	N/A	The required

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		least, identify and describe:				documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-3	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-3	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-3	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-3	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-3	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.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
CIP-005-3	R3.	Monitoring Electronic Access — The Responsible Entity shall implement	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-3	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.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at one or more access points to dial-up devices.
CIP-005-3	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.	N/A	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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-005-3	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 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 R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-3	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-3	R4.2.	A review to verify that only ports and services required for operations at these access	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		points are enabled;				
CIP-005-3	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-3	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-3	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.	N/A	N/A	N/A	N/A
CIP-005-3	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
CIP-005-3	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
CIP-005-3	R5.2.	The Responsible Entity shall update	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the documentation to reflect the modification of the network or controls within ninety calendar days of the change.				Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-3	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-008-3.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-006-3a	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security plan.	The Responsible Entity did not document, implement, and maintain a physical security plan.
CIP-006-3a	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security	N/A	N/A	N/A	The Responsible Entity's physical security plan does

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.				not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed or documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.
CIP-006-3a	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter or does not identify measures to control entry at those

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						access points.
CIP-006-3a	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-3a	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-3a	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the review of access authorization requests or the revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
CIP-006-3a	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	N/A	N/A	N/A	The Responsible Entity did not include or implement a visitor control program in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						its physical security plan or it does not meet the requirements of continuous escort.
CIP-006-3a	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-3a	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	N/A	N/A	N/A	N/A
CIP-006-3a	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address r updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						completion of a physical security system redesign or reconfiguration
CIP-006-3a	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-3a	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A	N/A	N/A	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was not afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
CIP-006-3a	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-3a	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	N/A	N/A	N/A	N/A
CIP-006-3a	R3	Protection of Electronic Access	N/A	N/A	N/A	A Cyber Assets used

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.				in the access control and/or monitoring of the Electronic Security Perimeter(s) does not reside within an identified Physical Security Perimeter.
CIP-006-3a	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or	N/A	N/A	N/A	The Responsible Entity has not documented or has 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 one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets				These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-3a	R5	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	N/A	N/A.	N/A	The Responsible Entity **has not documented or has not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.				Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						handled in accordance with CIP- 008-3.
CIP-006-3a	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4		N/A	N/A	The Responsible Entity **has not implemented or has not documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.
CIP-006-3a	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	N/A	N/A	N/A	The responsible entity did not retain physical access logs for at least ninety calendar days.
CIP-006-3a	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a	N/A	N/A	N/A	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		minimum, the following:				systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-3a	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-3a	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-3a	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-007-3	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-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of	N/A	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		operating systems, applications, database platforms, or other third-party software or firmware.				address one or more of the following: R1.1, R1.2, R1.3.
CIP-007-3	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.	N/A	N/A	N/A	N/A
CIP-007-3	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-3	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-3	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A	N/A	The Responsible Entity did not establish (implement) or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
CIP-007-3	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Perimeter(s).
CIP-007-3	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).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	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.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk.
CIP-007-3	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic	N/A	N/A	N/A	The Responsible Entity **did not establish (implement) or did not document**, either separately or as a component of the documented configuration management process specified in CIP-003-3

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Security Perimeter(s).				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-007-3	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.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-3	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk.
CIP-007-3	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).	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-3	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-3	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.	N/A	N/A	N/A	The Responsible Entity **did not document or did not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-3	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	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-3	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	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		respect to work functions performed.				authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
CIP-007-3	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
CIP-007-3	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.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-3	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R5 and Standard CIP-004-3 Requirement R4.
CIP-007-3	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.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
CIP-007-3	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.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-3	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-3	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).	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity 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-007-3	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-3	R5.3.1.	Each password shall be a minimum	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		of six characters.				
CIP-007-3	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-3	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-3	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.	N/A	N/A	N/A	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 on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	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.	N/A	N/A	N/A	The Responsible Entity **did not implement or 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.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-3	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-3	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-008-3.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
CIP-007-3	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-3	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-3	R7.	Disposal or Redeployment — The	N/A	N/A	The Responsible	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Responsible Entity shall establish and implement 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-005-3.			Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005- 3 **but** did not address redeployment as specified in R7.2.	Entity did not establish or implement 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-005-3. 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-005-2 but did not address disposal as specified in R7.1. OR The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Entity did not maintain records pertaining to disposal or[3] redeployment as specified in R7.3.
CIP-007-3	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.	N/A	N/A	N/A	N/A
CIP-007-3	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.	N/A	N/A	N/A	N/A
CIP-007-3	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-3	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment on one or more Cyber Assets within the Electronic Security Perimeter at least

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						annually. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
CIP-007-3	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-3	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;	N/A	N/A	N/A	N/A
CIP-007-3	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-3	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.	N/A	N/A	N/A	N/A
CIP-007-3	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 at least annually. OR The Responsible Entity did not document changes	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 at least annually **and** changes resulting from modifications to the systems or controls were not documented within

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	thirty calendar days of the change being completed.
CIP-008-3	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity has developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with those components.	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6, or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-3	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-3	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-3	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	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the ES-ISAC either directly or through an intermediary.				
CIP-008-3	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	N/A	N/A	N/A	N/A
CIP-008-3	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-3	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-3	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.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-009-3	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:	N/A	N/A	N/A	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 address

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						one or more of the requirements CIP-009-1 R1.1 **and** R1.2.
CIP-009-3	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-3	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-3	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-3	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 thirty calendar days of the change being completed.	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						an actual incident but the updates were not communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change.
CIP-009-3	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-3	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.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-3	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	MEDIUM
CIP-002-3	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	LOWER
CIP-002-3	R1.2	The risk-based assessment shall consider the following assets:	MEDIUM
CIP-002-3	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-002-3	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-3	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-3	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-002-3	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-002-3	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-3	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-002-3	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.	HIGH
CIP-002-3	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible 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	HIGH

Standard Number	Requirement Number	Text of Requirement	VRF
		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-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	
CIP-002-3	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	LOWER
CIP-002-3	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	LOWER
CIP-002-3	R3.3.	The Cyber Asset is dial-up accessible.	LOWER
CIP-002-3	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, 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 risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	LOWER
CIP-003-3	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:	MEDIUM
CIP-003-3	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.	LOWER
CIP-003-3	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-003-3	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-3	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-002-3 through CIP-009-3.	MEDIUM
CIP-003-3	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-3	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-3	R2.3.	Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-3	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-3	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).	LOWER
CIP-003-3	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-003-3	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOWER
CIP-003-3	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-003-3	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-3	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-002-3, 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.	MEDIUM
CIP-003-3	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-003-3	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-003-3	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-3	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-003-3	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	LOWER
CIP-003-3	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-3	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

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-3	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-3	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.	LOWER
CIP-004-3	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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-004-3	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOWER
CIP-004-3	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MEDIUM
CIP-004-3	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-3	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-3	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-3	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-3	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-3	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-004-3	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	
CIP-004-3	R3.1.	The Responsible Entity shall ensure that each assessment 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.	LOWER
CIP-004-3	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-004-3	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-004-3.	LOWER
CIP-004-3	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-004-3	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-004-3	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
CIP-005-3	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-005-3	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).	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-3	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.	MEDIUM
CIP-005-3	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).	MEDIUM
CIP-005-3	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-005-3.	MEDIUM
CIP-005-3	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	MEDIUM
CIP-005-3	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-005-3	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).	MEDIUM
CIP-005-3	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-005-3	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-005-3	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-3	R2.5.1.	The processes for access request and authorization.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-3	R2.5.2.	The authentication methods.	LOWER
CIP-005-3	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.	LOWER
CIP-005-3	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-3	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
CIP-005-3	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.	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	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:	MEDIUM
CIP-005-3	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-3	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-3	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-3	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-3	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.	LOWER
CIP-005-3	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-005-3	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-008-3.	LOWER
CIP-006-3	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-3	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-3	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-3	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-3	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-3	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	MEDIUM
CIP-006-3	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	MEDIUM
CIP-006-3a	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	MEDIUM
CIP-006-3a	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	MEDIUM
CIP-006-3	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-3	R1.8	Annual review of the physical security plan.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-3	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM
CIP-006-3	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-3	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	MEDIUM
CIP-006-3	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-3	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets	MEDIUM
CIP-006-3	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. - Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	
CIP-006-3	R6	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: - Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. - Video Recording: Electronic capture of video images of sufficient quality to determine identity. - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	LOWER
CIP-006-3	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	LOWER
CIP-006-3	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-3	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-3	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-3	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-3	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-007-3, a significant change shall, at a minimum, include implementation of security patches,	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	
CIP-007-3	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-007-3	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-3	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-3	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MEDIUM
CIP-007-3	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MEDIUM
CIP-007-3	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-007-3	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.	MEDIUM
CIP-007-3	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement 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-007-3	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-007-3	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.	LOWER
CIP-007-3	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).	MEDIUM
CIP-007-3	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	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	
CIP-007-3	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.	MEDIUM
CIP-007-3	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-007-3	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.	MEDIUM
CIP-007-3	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.	LOWER
CIP-007-3	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-007-3	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.	MEDIUM
CIP-007-3	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-007-3	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.	MEDIUM
CIP-007-3	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-3	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).	MEDIUM
CIP-007-3	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-3	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-3	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-3	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-3	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-007-3	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.	MEDIUM
CIP-007-3	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-3	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-008-3.	MEDIUM
CIP-007-3	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-3	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-3	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement 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-005-3.	LOWER
CIP-007-3	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-007-3	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-007-3	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-3	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-007-3	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-3	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;	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-3	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-3	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.	MEDIUM
CIP-007-3	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOWER
CIP-008-3	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOWER
CIP-008-3	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER
CIP-008-3	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	LOWER
CIP-008-3	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-008-3	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	LOWER
CIP-008-3	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-3	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-3	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
CIP-009-3	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-009-3	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-009-3	R1.2.	Define the roles and responsibilities of responders.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-009-3	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-009-3	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 thirty calendar days of the change being completed.	LOWER
CIP-009-3	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-009-3	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

CIP Version 3 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-3	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
CIP-002-3	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
CIP-002-3	R1.2	The risk-based assessment shall consider the following assets:	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.
CIP-002-3	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-3	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	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.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	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.	N/A	N/A	N/A	N/A
CIP-002-3	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.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-3	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:			Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	operation of the Critical Asset list as per requirement R2 even if such list is null.
CIP-002-3	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R3.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	A Cyber Asset

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, 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 risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets **or** the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-3	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,	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security policy.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		at minimum, ensure the following:				
CIP-003-3	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-3	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-3	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-3	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-002-3 through CIP-009-3.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-3	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	~~The senior manager is not identified by name, title, and date of designation.~~ Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-3	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
CIP-003-3	R2.3.	Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager,	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.
CIP-003-3	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-3	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).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, 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, in R1, exceptions were not documented.
CIP-003-3	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).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						approved by the senior manager or delegate(s).
CIP-003-3	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	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.	The Responsible Entity has a documented exception to the cyber security policy in R1~~(pertaining to CIP 002 through CIP 009)~~ but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-3	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.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved 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-003-3	R4.	Information Protection — The Responsible Entity shall implement	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and document a program to identify, classify, and protect information associated with Critical Cyber Assets.				implement or did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-3	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-002-3, 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.	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.
CIP-003-3	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-3	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.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						documentation of the assessment results, OR The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-3	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.
CIP-003-3	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-3	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, and the information for	Personnel are not identified by name, title, or the information for which they are

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					which they are responsible for authorizing access, but the business phone is missing.	responsible for authorizing access.
CIP-003-3	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-3	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.	N/A	N/A	N/A	The Responsible Entity did not 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.
CIP-003-3	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						information.
CIP-003-3	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.	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-004-3	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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	N/A~~The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security~~	N/A~~The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security~~	The Responsible Entity did not establish, implement, maintain, ~~n~~or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	~~practices.~~		~~practices.~~ The Responsible[1] Entity did not provide security awareness reinforcement on at least a quarterly basis.	practices.
CIP-004-3	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	N/A~~The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~	N/A~~The Responsibility Entity did not review the training program on an annual basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~ The Responsible[2] Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, ~~n~~or document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-3	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted	N/A~~At least one individual but less than 5% of personnel having authorized cyber or~~	N/A~~At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical~~	N/A~~At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical~~	~~15% or more of~~ Not all personnel having authorized cyber or unescorted physical access to Critical

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		such access except in specified circumstances such as an emergency.	~~unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	~~access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	~~access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	Cyber Assets, including contractors and service vendors, were ~~not~~ trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-3	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-3	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-3	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.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not	The Responsible Entity did not maintain documentation that training is conducted at least

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					include attendance records.	annually, including the date the training was completed and attendance records.
CIP-004-3	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	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 after such personnel were granted such access except in specified circumstances such as an emergency.	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 except in specified

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						circumstances such as an emergency.
CIP-004-3	R3.1.	The Responsible Entity shall ensure that each assessment 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.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-3	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.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-3	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-	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		004-3.	authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-3	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.	The Responsible Entity did not maintain complete 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, missing at least one individual but less than 5% of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 10% or more but less than 15%of the authorized personnel.	The Responsible Entity did not maintain complete 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, missing 15% or more of the authorized personnel.
CIP-004-3	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	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		properly maintained.				with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-3	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.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.
CIP-005-3	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).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-3	R1.1.	Access points to the Electronic Security Perimeter(s) shall include	N/A	N/A	N/A	Access points to the Electronic Security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).				Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-3	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.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
CIP-005-3	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).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-3	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-005-3.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-3	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3, Standard CIP-007-3 Requirements R1 and R3 through R9;, Standard CIP-008-3;~~	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3;, Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9;, Standard CIP-008-3;~~	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3;~~	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded ~~is not provided without four (4)~~ one (1) or more of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3c Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~and Standard CIP-009-3.~~	~~and Standard CIP-009-3.~~	~~and Standard CIP-009-3.~~	009-3.
CIP-005-3	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.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of 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-005-3	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).	N/A	N/A	N/A	The Responsible Entity did not implement or did not document the organizational processes and technical and procedural mechanisms for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
CIP-005-3	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.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-3	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.	N/A	N/A	N/A	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, or did not document, individually or by specified grouping, the configuration of those ports and services.
CIP-005-3	R2.3.	The Responsible Entity shall implement and maintain a	N/A	N/A	N/A~~The Responsible Entity did~~	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		procedure for securing dial-up access to the Electronic Security Perimeter(s).			~~implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.~~	implement ~~n~~or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-3	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.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-3	R2.5.	The required documentation shall, at least, identify and describe:	N/A	N/A	N/A	The required documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-3	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-3	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-3	R2.5.3.	The review process for authorization rights, in accordance with Standard	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		CIP-004-3 Requirement R4.				
CIP-005-3	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-3	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.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
CIP-005-3	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.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-3	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	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access point to the dial-up device, where technically feasible.				electronic or manual processes for monitoring at one or more access points to dial-up devices.
CIP-005-3	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.	N/A	N/A	N/A	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.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-3	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 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 R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-3	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-3	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-3	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-3	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-3	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.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-3	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
CIP-005-3	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
CIP-005-3	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.	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-3	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to	The Responsible Entity retained	The Responsible Entity retained	The Responsible Entity retained	The Responsible Entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	retained electronic access logs for less than 45 calendar days.
CIP-006-3a	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security plan.	The Responsible Entity did not document, implement, and maintain a physical security plan.
CIP-006-3a	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	N/A~~Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	N/A~~Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed ~~and~~ or documented alternative measures to control physical access to ~~the Critical s~~ such Cyber Assets within the Electronic Security Perimeter.
CIP-006-3a	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A~~The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.~~	N/A~~The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.~~	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter ~~n~~or does not identify measures to control entry at those access points.
CIP-006-3a	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-3a	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-3a	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	N/A	N/A	N/A~~The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.~~	The Responsible Entity's physical security plan does not address the ~~process for~~ review~~ing~~ of access authorization requests ~~and~~ or the ~~process for~~ revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
CIP-006-3a	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	N/A~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.~~	~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~N/A	N/A~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~	The Responsible Entity did not include or implement a visitor control program in its physical security plan or it does not meet the requirements of continuous escort.~~.~~

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-3a	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-3a	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	N/A	N/A	N/A	N/A
CIP-006-3a	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	N/A~~The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration **but** the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.~~	The Responsible Entity's physical security plan does not address ~~a process fo~~r updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration
CIP-006-3a	R1.8	Annual review of the physical	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		security plan.				Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-3a	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and~~	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and~~	~~A~~N/A~~ Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and~~	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Standard CIP-009-3.~~	~~Standard CIP-009-3.~~	~~Standard CIP-009-3.~~	point such as electronic lock control mechanisms and badge readers was ~~provided without~~ not afforded ~~four (4) or more of~~ the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
CIP-006-3a	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-3a	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	N/A	N/A	N/A	N/A
CIP-006-3a	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Perimeter(s) shall reside within an identified Physical Security Perimeter.				Security Perimeter(s) ~~did~~ does not reside within an identified Physical Security Perimeter.
CIP-006-3a	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication	N/A	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 one or more of the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to,~~	N/A~~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 one or more of the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to,~~	The Responsible Entity has not documented ~~n~~or has 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 one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets		~~locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.~~	~~locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.~~	locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-3a	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following	N/A	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) twenty-four hours a~~	N/A~~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) twenty-four hours a~~	The Responsible Entity **has not documented** ~~**n**~~**or** has not **implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.		~~day, seven days a week using one or more of the following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.~~ ~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4~~.	~~day, seven days a week using one or more of the following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.~~ ~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~	twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						accordance with CIP- 008-3.
CIP-006-3a	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	~~The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical~~	N/A~~The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained~~	N/A~~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 following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical~~	The Responsible Entity **has not implemented ~~n~~or has not documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.~~	~~by security or other personnel authorized to control and monitor physical access as specified in Requirement R4,~~ ~~**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.~~	~~access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.~~	record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.
CIP-006-3a	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	N/A~~The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.~~	N/A~~The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.~~	N/A~~The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.~~	~~The Responsible Entity retained physical access logs for less than 45 calendar days.~~ The responsible entity did not retain physical access logs for at least ninety calendar days.
CIP-006-3a	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security	N/A~~The Responsible Entity has implemented a maintenance and~~	N/A~~The Responsible Entity has implemented a maintenance and~~	N/A~~The Responsible Entity has implemented a maintenance and~~	The Responsible Entity has not implemented a maintenance and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	~~testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include one of the Requirements R8.1, R8.2, and R8.3.~~	~~testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include two of the Requirements R8.1, R8.2, and R8.3.~~	~~testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include any of the Requirements R8.1, R8.2, and R8.3.~~	testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-3a	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-3a	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-3a	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-007-3	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-007-3, a significant change shall, at a minimum, include	N/A	N/A	N/A	The Responsible Entity did not ensure the prevention of adverse affects described in R1, by not including the required minimum significant changes.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				OR The Responsible Entity did not address one or more of the following: R1.1, R1.2, R1.3.
CIP-007-3	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.	N/A	N/A	N/A	N/A
CIP-007-3	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-3	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-3	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A~~The Responsible Entity **established (implemented) but did not document** a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	N/A~~The Responsible Entity **documented but did not establish (implement)** a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	The Responsible Entity did not establish (implement) ~~n~~or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
CIP-007-3	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	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).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	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.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk. ~~exposure or state an acceptance of risk.~~
CIP-007-3	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall	N/A~~The Responsible Entity established (implemented) and documented, either separately or as a component of~~	N/A~~The Responsible Entity **established (implemented) but did not document**, either separately or as a component of~~	N/A~~The Responsible Entity **documented but did not establish (implement)**, either separately or as a~~	The Responsible Entity **did not establish (implement)** ~~n~~**or** did not **document**, either separately or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		establish, document and implement 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 documented configuration management process specified in CIP-003-3 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 documented configuration management process specified in CIP-003-3 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).~~	~~component of the documented configuration management process specified in CIP-003-3 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).~~	as a component of the documented configuration management process specified in CIP-003-3 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-007-3	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.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-3	R3.2.	The Responsible Entity shall document the implementation of	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.				document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk. ~~exposure or an acceptance of risk.~~
CIP-007-3	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).	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-3	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)	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		applied to mitigate risk exposure.				assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-3	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.	N/A	N/A	N/A	The Responsible Entity **did not document or did not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-3	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,	N/A	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and that minimize the risk of unauthorized system access.				enforce access authentication of, and accountability for, all user activity.
CIP-007-3	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.	N/A	N/A	N/A	The Responsible Entity did not 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-007-3	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
CIP-007-3	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.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				days.		
CIP-007-3	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
CIP-007-3	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.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
CIP-007-3	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.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					to putting any system into service.	
CIP-007-3	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-3	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).	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity 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-007-3	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-3	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-3	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and "special" characters.	N/A	N/A	N/A	N/A
CIP-007-3	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-3	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.	N/A	N/A	N/A	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 on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	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	N/A	N/A	N/A	The Responsible Entity **did not implement or did not document** the organizational processes and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		within the Electronic Security Perimeter.				technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
CIP-007-3	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-3	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-008-3.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
CIP-007-3	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-3	R6.5.	The Responsible Entity shall review	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		logs of system events related to cyber security and maintain records documenting review of logs.				Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-3	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement 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-005-3.	N/A~~The Responsible Entity established and implemented 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-005-3~~ ~~**but** did not maintain records as specified in R7.3.~~	N/A~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005- 3~~ ~~**but** did not address redeployment as specified in R7.2.~~	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005- 3 **but** did not address ~~disposal~~ redeployment as specified in R7.2~~1~~.	The Responsible Entity did not establish or implement 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-005-3. 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 Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Standard CIP-005-2 but did not address disposal as specified in R7.1. OR The Responsible Entity did not maintain records pertaining to disposal or[3] redeployment as specified in R7.3.
CIP-007-3	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.	N/A	N/A	N/A	N/A
CIP-007-3	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.	N/A	N/A	N/A	N/A
CIP-007-3	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-3	R8	Cyber Vulnerability Assessment —	N/A	N/A	N/A	The Responsible

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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:				Entity did not perform a Vulnerability Assessment 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-007-3	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-3	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;	N/A	N/A	N/A	N/A
CIP-007-3	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-3	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.	N/A	N/A	N/A	N/A
CIP-007-3	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes	N/A	N/A	The Responsible Entity did not review and update the documentation specified in	The Responsible Entity did not review and update the documentation specified in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.			Standard CIP-007-3 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	Standard CIP-007-3 at least annually ~~nor~~ and ~~were~~ changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being completed.
CIP-008-3	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	N/A~~The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.~~	The Responsible Entity has developed a Cyber Security Incident response plan ~~but the plan~~that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with those components. ~~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 of the components required by R1.1 through R1.6, or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-3	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-008-3	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-3	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.	N/A	N/A	N/A	N/A
CIP-008-3	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	N/A	N/A	N/A	N/A
CIP-008-3	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-3	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-3	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.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						for at least three calendar years.
CIP-009-3	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:	N/A	N/A	N/A	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 address one or more of the requirements CIP-009-1 R1.1 **and** R1.2.
CIP-009-3	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-3	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-3	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-3	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	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~~	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~~	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~~	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		plan(s) within thirty calendar days of the change being completed.	~~an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than30 but less than or equal to 120 calendar days of the change.~~	~~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.~~	~~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.~~	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 thirty ~~more than 180~~ calendar days of the change.
CIP-009-3	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-009-3	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.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-3	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	MEDIUM
CIP-002-3	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	LOWER
CIP-002-3	R1.2	The risk-based assessment shall consider the following assets:	MEDIUM
CIP-002-3	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-002-3	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-3	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-3	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-002-3	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-002-3	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-3	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-002-3	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.	HIGH
CIP-002-3	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible 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-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	HIGH
CIP-002-3	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	LOWER
CIP-002-3	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	LOWER
CIP-002-3	R3.3.	The Cyber Asset is dial-up accessible.	LOWER
CIP-002-3	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, 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 risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	LOWER
CIP-003-3	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:	MEDIUM
CIP-003-3	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-3 through	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		CIP-009-3, including provision for emergency situations.	
CIP-003-3	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-003-3	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-3	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-002-3 through CIP-009-3.	~~LOWER~~MEDIUM
CIP-003-3	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-3	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-3	R2.3.	Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-3	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-3	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).	LOWER
CIP-003-3	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-003-3	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOWER
CIP-003-3	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-003-3	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-3	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-002-3, 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.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-3	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-003-3	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-003-3	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-3	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-003-3	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	LOWER
CIP-003-3	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-3	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-003-3	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-3	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.	LOWER
CIP-004-3	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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-004-3	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-004-3	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MEDIUM
CIP-004-3	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-3	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-3	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-3	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-3	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-3	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-004-3	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	MEDIUM
CIP-004-3	R3.1.	The Responsible Entity shall ensure that each assessment 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.	LOWER
CIP-004-3	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-004-3	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-004-3.	LOWER
CIP-004-3	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

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-004-3	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-004-3	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
CIP-005-3	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-005-3	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).	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	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).	MEDIUM
CIP-005-3	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-005-3.	MEDIUM
CIP-005-3	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	MEDIUM
CIP-005-3	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-005-3	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).	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-3	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-005-3	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-005-3	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-3	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-3	R2.5.2.	The authentication methods.	LOWER
CIP-005-3	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.	LOWER
CIP-005-3	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-3	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
CIP-005-3	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.	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	
CIP-005-3	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-3	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-3	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-3	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	MEDIUM
CIP-005-3	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.	MEDIUM
CIP-005-3	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	LOWER
CIP-005-3	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.	LOWER
CIP-005-3	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-005-3	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-008-3.	LOWER
CIP-006-3	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-3	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-3	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-3	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-3	R1.4	Appropriate use of physical access controls as described in Requirement R4 including	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	
CIP-006-3	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	MEDIUM
CIP-006-3	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	MEDIUM
CIP-006-3a	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	MEDIUM
CIP-006-3a	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	MEDIUM
CIP-006-3	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-3	R1.8	Annual review of the physical security plan.	LOWER
CIP-006-3	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM
CIP-006-3	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-3	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	MEDIUM
CIP-006-3	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MEDIUM
CIP-006-3	R4	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: • 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	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets	
CIP-006-3	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-3	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	LOWER
CIP-006-3	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		accordance with the requirements of Standard CIP-008-3.	
CIP-006-3	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-3	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-3	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-3	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-3	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-007-3, 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-007-3	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-007-3	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-3	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-3	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MEDIUM
CIP-007-3	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MEDIUM
CIP-007-3	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-007-3	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.	MEDIUM
CIP-007-3	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		3 Requirement R6, shall establish, document and implement 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-007-3	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-007-3	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.	LOWER
CIP-007-3	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).	MEDIUM
CIP-007-3	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.	MEDIUM
CIP-007-3	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.	MEDIUM
CIP-007-3	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-007-3	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.	MEDIUM
CIP-007-3	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.	LOWER
CIP-007-3	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-007-3	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.	MEDIUM
CIP-007-3	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	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		factory default accounts.	
CIP-007-3	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.	MEDIUM
CIP-007-3	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-3	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).	MEDIUM
CIP-007-3	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-3	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-3	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-3	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-3	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-007-3	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.	MEDIUM
CIP-007-3	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-3	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-008-3.	MEDIUM
CIP-007-3	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-3	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-3	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement 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-005-3.	LOWER
CIP-007-3	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	
CIP-007-3	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-007-3	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-3	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-007-3	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-3	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;	MEDIUM
CIP-007-3	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-3	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.	MEDIUM
CIP-007-3	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOWER
CIP-008-3	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOWER
CIP-008-3	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER
CIP-008-3	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	LOWER
CIP-008-3	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-008-3	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	LOWER
CIP-008-3	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		annually.	
CIP-008-3	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-3	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
CIP-009-3	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-009-3	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-009-3	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-3	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-009-3	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 thirty calendar days of the change being completed.	LOWER
CIP-009-3	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-009-3	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

EXHIBIT D

CIP VIOLATION RISK FACTORS AND VIOLATION SEVERITY LEVELS – VERSION 4
(CLEAN AND REDLINE)

CIP Version 4 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-4	R1.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-4	R2.	Critical Cyber Asset Identification—Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1. For the purpose of Standard CIP 002-4, Critical Cyber Assets are further qualified to be those having at least	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber Asset List.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.				
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 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.)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-4	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	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Assets. The Responsible Entity shall, at minimum, ensure the following:				policy.
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-4	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-4	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-4	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-002-4 through CIP-009-4.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager;

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					Changes to the delegated authority are not documented within thirty calendar days of the effective date.	AND changes to the delegated authority are not documented within thirty calendar days of the effective date.
CIP-003-4	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-4	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).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, 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, in R1, exceptions were not documented.
CIP-003-4	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).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						delegate(s).
CIP-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not include **either**: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-4	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.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved 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-003-4	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						information associated with Critical Cyber Assets.
CIP-003-4	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-002-4, 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.	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.
CIP-003-4	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	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.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-4	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.
CIP-003-4	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, and the information for which they are responsible for authorizing access, but the business	Personnel are not identified by name, title, or the information for which they are responsible for authorizing access.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					phone is missing.	
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-4	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.	N/A	N/A	N/A	The Responsible Entity did not 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.
CIP-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-4	R6.	Change Control and Configuration Management — The Responsible	N/A	N/A	N/A	The Responsible Entity has not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-004-4	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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	N/A	N/A	The Responsible[[1]] Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).				practices.
CIP-004-4	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	N/A	N/A	The Responsible[[2]] Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, or document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A	N/A	N/A	Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were trained prior to their being granted such access except in specified circumstances such as an emergency.

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-4	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.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
CIP-004-4	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	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R3, for personnel having authorized	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk	The Responsible Entity does not have a documented personnel risk assessment program, as stated in R3, for personnel

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:		cyber or authorized unescorted physical access, but the program is not documented.	assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	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 except in specified circumstances such as an emergency.
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment 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.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-4	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.	N/A	The Responsible Entity did not update each personnel risk assessment at least	The Responsible Entity did not update each personnel risk assessment for	The Responsible Entity did not update each personnel risk assessment at least

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				every seven years after the initial personnel risk assessment but did update it for cause when applicable.	cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-4	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-004-4.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-4	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.	The Responsible Entity did not maintain complete 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	The Responsible Entity did not maintain complete 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	The Responsible Entity did not maintain complete 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	The Responsible Entity did not maintain complete 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	Cyber Assets, missing 10% or more but less than 15%of the authorized personnel.	Cyber Assets, missing 15% or more of the authorized personnel.
CIP-004-4	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.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-4	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.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-4	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).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-4	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).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-4	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.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Perimeter for that single access point at the dial-up device.
CIP-005-4	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).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-4	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-005-4.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-4	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2	N/A	N/A	N/A	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded one (1) or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.				more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4c Requirements R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.
CIP-005-4	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.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						access control and monitoring of these access points.
CIP-005-4	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).	N/A	N/A	N/A	The Responsible Entity did not implement or 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-005-4	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.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-4	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,	N/A	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the configuration of those ports and services.				monitoring Cyber Assets within the Electronic Security Perimeter, or did not document, individually or by specified grouping, the configuration of those ports and services.
CIP-005-4	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not implement or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-4	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.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-4	R2.5.	The required documentation shall, at	N/A	N/A	N/A	The required

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		least, identify and describe:				documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-4	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-4	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.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
CIP-005-4	R3.	Monitoring Electronic Access — The Responsible Entity shall implement	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-4	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.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at one or more access points to dial-up devices.
CIP-005-4	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.	N/A	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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-005-4	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 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 R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-4	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-4	R4.2.	A review to verify that only ports and services required for operations at these access	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		points are enabled;				
CIP-005-4	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-4	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-4	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.	N/A	N/A	N/A	N/A
CIP-005-4	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
CIP-005-4	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
CIP-005-4	R5.2.	The Responsible Entity shall update	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the documentation to reflect the modification of the network or controls within ninety calendar days of the change.				Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-4	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-008-4.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-006-4c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security plan.	The Responsible Entity did not document, implement, and maintain a physical security plan.
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security	N/A	N/A	N/A	The Responsible Entity's physical security plan does

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.				not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed or documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter or does not identify measures to control entry at those

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						access points.
CIP-006-4c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-4c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-4c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the review of access authorization requests or the revocation of access authorization, in accordance with CIP-004-4 Requirement R4.
CIP-006-4c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	N/A	N/A	N/A	The Responsible Entity did not include or implement a visitor control program in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						its physical security plan or it does not meet the requirements of continuous escort.
CIP-006-4c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	N/A	N/A	N/A	N/A
CIP-006-4c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address r updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						a physical security system redesign or reconfiguration
CIP-006-4c	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-4c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A	N/A	N/A	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s),

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was not afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4a Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	N/A	N/A	N/A	N/A
CIP-006-4c	R3	Protection of Electronic Access Control Systems — Cyber Assets	N/A	N/A	N/A	A Cyber Assets used in the access control

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.				and/or monitoring of the Electronic Security Perimeter(s) does not reside within an identified Physical Security Perimeter.
CIP-006-4c	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	N/A	N/A	N/A	The Responsible Entity has not documented or has 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 one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets				are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-4c	R5	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-008-4.	N/A	N/A.	N/A	The Responsible Entity **has not documented or has not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.				twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						handled in accordance with CIP-008-4.
CIP-006-4c	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4		N/A	N/A	The Responsible Entity **has not implemented or has not documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.
CIP-006-4c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	N/A	N/A	N/A	The responsible entity did not retain physical access logs for at least ninety calendar days.
CIP-006-4c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-4c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-007-4	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-007-4, 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-	N/A	N/A	N/A	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:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		party software or firmware.				R1.1, R1.2, R1.3.
CIP-007-4	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.	N/A	N/A	N/A	N/A
CIP-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-4	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A	N/A	The Responsible Entity did not establish (implement) or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	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).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	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.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk.
CIP-007-4	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement 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).	N/A	N/A	N/A	The Responsible Entity **did not establish (implement) or did not document**, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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-007-4	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.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk.
CIP-007-4	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).	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity **did not document or did not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-4	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	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-4	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	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		performed.				permissions are consistent with the concept of "need to know" with respect to work functions performed.
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
CIP-007-4	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.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R5 and Standard CIP-004-4 Requirement R4.
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
CIP-007-4	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.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-4	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall	N/A	N/A	N/A	Where such

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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).				accounts must be shared, the Responsible Entity 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-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and "special" characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-4	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.	N/A	N/A	N/A	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 on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity **did not implement or 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.
CIP-007-4	R6.2.	The security monitoring controls	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall issue automated or manual alerts for detected Cyber Security Incidents.				entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-4	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-008-4.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish	N/A	N/A	The Responsible Entity established	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and implement 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-005-4.			and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.	establish or implement 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-005-4. 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-005-4 but did not address disposal as specified in R7.1. OR The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						maintain records pertaining to disposal or[3] redeployment as specified in R7.3.
CIP-007-4	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.	N/A	N/A	N/A	N/A
CIP-007-4	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.	N/A	N/A	N/A	N/A
CIP-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-4	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment on one or more Cyber Assets within the Electronic Security Perimeter at least annually.

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
CIP-007-4	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-4	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;	N/A	N/A	N/A	N/A
CIP-007-4	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-4	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.	N/A	N/A	N/A	N/A
CIP-007-4	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually **and** changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					systems or controls within thirty calendar days of the change being completed.	completed.
CIP-008-4	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity has developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with those components.	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6, or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-4	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.	N/A	N/A	N/A	N/A
CIP-008-4	R1.4.	Process for updating the Cyber	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Security Incident response plan within thirty calendar days of any changes.				
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-4	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.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-009-4	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:	N/A	N/A	N/A	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 address one or more of the requirements CIP-009-4 R1.1 **and** R1.2.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-009-4	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-4	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-4	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-4	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 thirty calendar days of the change being completed.	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						were not communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change.
CIP-009-4	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-4	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.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-4	R1.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.	HIGH
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion For the purpose of Standard CIP 002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.	HIGH
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 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	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	
CIP-003-4	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:	MEDIUM
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	LOWER
CIP-003-4	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-003-4	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-4	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-002-4 through CIP-009-4.	MEDIUM
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-4	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-4	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).	LOWER
CIP-003-4	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-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOWER
CIP-003-4	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

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-4	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-4	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-002-4, 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.	MEDIUM
CIP-003-4	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-003-4	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-003-4	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-4	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-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	LOWER
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-4	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-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-4	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.	LOWER
CIP-004-4	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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:	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		- 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.).	
CIP-004-4	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOWER
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MEDIUM
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-4	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-004-4	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	MEDIUM
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment 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.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-004-4	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-004-4	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-004-4.	LOWER
CIP-004-4	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-004-4	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-004-4	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
CIP-005-4	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-005-4	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).	MEDIUM
CIP-005-4	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.	MEDIUM
CIP-005-4	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).	MEDIUM
CIP-005-4	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-005-4.	MEDIUM
CIP-005-4	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		through R9; Standard CIP-008-4; and Standard CIP-009-4.	
CIP-005-4	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-005-4	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).	MEDIUM
CIP-005-4	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-005-4	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-005-4	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	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.	MEDIUM
CIP-005-4	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-4	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-4	R2.5.2.	The authentication methods.	LOWER
CIP-005-4	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	LOWER
CIP-005-4	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-4	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
CIP-005-4	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.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-4	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.	MEDIUM
CIP-005-4	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.	MEDIUM
CIP-005-4	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:	MEDIUM
CIP-005-4	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-4	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-4	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-4	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	MEDIUM
CIP-005-4	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.	MEDIUM
CIP-005-4	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.	LOWER
CIP-005-4	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.	LOWER
CIP-005-4	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-005-4	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-008-4.	LOWER
CIP-006-4c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-4c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-4c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-4c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	MEDIUM
CIP-006-4c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	MEDIUM
CIP-006-4c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	MEDIUM
CIP-006-4c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	MEDIUM
CIP-006-4c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-4c	R1.8	Annual review of the physical security plan.	LOWER
CIP-006-4c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4a Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	MEDIUM
CIP-006-4c	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		identified Physical Security Perimeter.	
CIP-006-4c	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets	MEDIUM
CIP-006-4c	R5	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-008-4. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-4c	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		selected access control and monitoring method. - Video Recording: Electronic capture of video images of sufficient quality to determine identity. - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	
CIP-006-4c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	LOWER
CIP-006-4c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-4c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-4c	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-4c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-4	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-007-4, 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-007-4	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-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-4	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MEDIUM
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		and emergency operations.	
CIP-007-4	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-007-4	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.	MEDIUM
CIP-007-4	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement 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-007-4	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-007-4	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.	LOWER
CIP-007-4	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).	MEDIUM
CIP-007-4	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.	MEDIUM
CIP-007-4	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.	MEDIUM
CIP-007-4	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-007-4	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.	MEDIUM
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		designated personnel. Refer to Standard CIP-003-4 Requirement R5.	
CIP-007-4	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-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	MEDIUM
CIP-007-4	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-007-4	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.	MEDIUM
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-4	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).	MEDIUM
CIP-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-4	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-007-4	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.	MEDIUM
CIP-007-4	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-4	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-008-4.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement 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-005-4.	LOWER
CIP-007-4	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-007-4	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-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-4	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-007-4	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-4	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;	MEDIUM
CIP-007-4	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-4	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.	MEDIUM
CIP-007-4	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOWER
CIP-008-4	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOWER
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	LOWER
CIP-008-4	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-008-4	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	LOWER
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-4	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
CIP-009-4	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-009-4	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-009-4	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-4	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-009-4	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 thirty calendar days of the change being completed.	LOWER
CIP-009-4	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-009-4	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

CIP Version 4 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-4	R1.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1. For the purpose of Standard CIP 002-4, Critical Cyber Assets are further qualified to be those having at least	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber Asset List.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.				
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 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.)	N/A	N/A~~The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)~~	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.) ~~The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual~~	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) ~~The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets,~~

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)~~	~~nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)~~
CIP-003-4	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:	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security policy.
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-4	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-4	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-002-4 through CIP-009-4.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	~~The senior manager is not identified by name, title, and date of designation.~~ Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						30 days of the effective date.
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.
CIP-003-4	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	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).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, 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, in R1, exceptions were not documented.
CIP-003-4	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).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).
CIP-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	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	The Responsible Entity has a documented exception to the cyber security policy in R1~~(pertaining to CIP 002 through CIP 009)~~ but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					measures.	
CIP-003-4	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.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved 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-003-4	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-4	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-002-4, 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.	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	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.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-4	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber Asset information.
CIP-003-4	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, 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.
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-4	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	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.				information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
CIP-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-4	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.	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R6.
CIP-004-4	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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.).	N/A~~The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~	N/A~~The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~ The Responsible[1] Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, ~~n~~or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
CIP-004-4	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The	N/A~~The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training~~	N/A~~The Responsibility Entity did not review the training program on an annual basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security~~	The Responsible Entity did not establish, implement, maintain, ~~n~~or document an annual cyber security

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	~~program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~		~~training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~ The Responsible[2] Entity did not review the training program on an annual basis.	training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A~~At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	N/A~~At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	N/A~~At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	~~15% or more of~~ Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were~~ not~~ trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3,

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		personnel roles and responsibilities:				R2.2.4.
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-4	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.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
CIP-004-4	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such	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	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:		authorized cyber or authorized unescorted physical access, but the program is not documented.	as an emergency.	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 except in specified circumstances such as an emergency.
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment 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.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-4	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or	N/A	The Responsible Entity did not update each personnel risk	The Responsible Entity did not update each personnel risk	The Responsible Entity did not update each personnel risk

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for cause.		assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-4	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-004-4.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-4	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.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			rights to Critical Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	rights to Critical Cyber Assets, missing 10% or more but less than 15%of the authorized personnel.	rights to Critical Cyber Assets, missing 15% or more of the authorized personnel.
CIP-004-4	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.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-4	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.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-4	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).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-4	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).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-4	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.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Perimeter for that single access point at the dial-up device.
CIP-005-4	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).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-4	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-005-4.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-4	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but~~	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but~~	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but~~	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded ~~is~~

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	~~one (1) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3, Standard CIP-007-3 Requirements R1 and R3 through R9;, Standard CIP-008-3; and Standard CIP-009-3.~~	~~two (2) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3;, Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9;, Standard CIP-008-3; and Standard CIP-009-3.~~	~~three (3) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.~~	~~not provided without four (4)~~ one (1) or more of the protective measures as specified in Standard CIP-003-4~~3~~; Standard CIP-004-4~~3~~ Requirement R3; Standard CIP-005-4~~3~~ Requirements R2 and R3; Standard CIP-006-4~~3~~c~~a~~ Requirements R3; Standard CIP-007-4~~3~~ Requirements R1 and R3 through R9; Standard CIP-008-4~~3~~; and Standard CIP-009-4~~3~~.
CIP-005-4	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.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of one or more of the following: Electronic Security Perimeter(s), interconnected Critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), electronic access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
CIP-005-4	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).	N/A	N/A	N/A	The Responsible Entity did not implement or 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-005-4	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.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-4	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services	N/A	N/A	N/A	At one or more access points to the Electronic Security Perimeter(s), the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, or did not document, individually or by specified grouping, the configuration of those ports and services.
CIP-005-4	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A~~The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.~~	The Responsible Entity did not implement ~~n~~or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-4	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.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						of the accessing party, where technically feasible.
CIP-005-4	R2.5.	The required documentation shall, at least, identify and describe:	N/A	N/A	N/A	The required documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-4	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-4	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.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			interactive access attempts.			
CIP-005-4	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.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-4	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.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at one or more access points to dial-up devices.
CIP-005-4	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.	N/A	N/A	N/A	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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-005-4	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 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 R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-4	R4.1.	A document identifying the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerability assessment process;				
CIP-005-4	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-4	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-4	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-4	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.	N/A	N/A	N/A	N/A
CIP-005-4	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
CIP-005-4	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						referenced in Standard CIP-005 at least annually.
CIP-005-4	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.	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-4	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-008-4.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-006-4c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security	The Responsible Entity did not document, implement, and maintain a physical security plan.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					plan.	
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	N/A~~Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	N/A~~Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed ~~and~~ or documented alternative measures to control physical access to ~~the Critical s~~ such Cyber Assets within the Electronic Security Perimeter.
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A~~The Responsible Entity's physical security plan includes measures to control entry at access points but~~	N/A~~The Responsible Entity's physical security identifies all access points through each Physical Security~~	The Responsible Entity's physical security plan does not identify all access points through each

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~does not identify all access points through each Physical Security Perimeter.~~	~~Perimeter but does not identify measures to control entry at those access points.~~	Physical Security Perimeter ~~n~~or does not identify measures to control entry at those access points.
CIP-006-4c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-4c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-4c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	N/A	N/A	N/A~~The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with~~	The Responsible Entity's physical security plan does not address the ~~process for~~ review~~ing~~ of access authorization requests ~~and~~ or the ~~process for~~ revocation of access authorization, in accordance with

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~CIP-004-3 Requirement R4.~~	CIP-004-4~~3~~ Requirement R4.
CIP-006-4c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	N/A~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.~~	~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~N/A	N/A~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~	The Responsible Entity did not include or implement a visitor control program in its physical security plan or it does not meet the requirements of continuous escort.~~.~~
CIP-006-4c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	N/A	N/A	N/A	N/A
CIP-006-4c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	N/A~~The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration **but** the plan was not~~	The Responsible Entity's physical security plan does not address ~~a process fo~~r updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.~~	completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration
CIP-006-4c	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-4c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with~~	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with~~	~~A~~N/A~~ Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with~~	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~all but one (1) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.~~	~~all but two (2) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.~~	~~all but three (3) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.~~	from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was ~~provided without~~ not afforded ~~four (4) or more of~~ the protective measures specified in Standard CIP-003-4~~3~~; Standard CIP-004-4~~3~~ Requirement R3; Standard CIP-005-4~~3~~ Requirements R2 and R3; Standard CIP-006-4c~~3a~~ Requirements R4 and R5; Standard CIP-007-4~~3~~; Standard CIP-008-4~~3~~; and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Standard CIP-009-4~~3~~.
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4a Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	N/A	N/A	N/A	N/A
CIP-006-4c	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) ~~did~~ does not reside within an identified Physical Security Perimeter.
CIP-006-4c	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a	N/A	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 one or more of~~	N/A~~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 one or more of~~	The Responsible Entity has not documented ~~n~~or has 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 one or more of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets		~~the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent~~	~~the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent~~	the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~devices that control physical access to the Critical Cyber Assets.~~	~~devices that control physical access to the Critical Cyber Assets.~~	devices that control physical access to the Critical Cyber Assets.
CIP-006-4c	R5	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-008-4. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	N/A	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) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:~~ ~~• 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.~~	N/A~~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) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:~~ ~~• 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.~~	The Responsible Entity **has not documented** ~~n~~**or** has not **implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4~~.	~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~	response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-4~~3~~.
CIP-006-4c	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and	~~The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized~~	N/A~~The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic~~	N/A~~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 following logging methods or their equivalent:~~ ~~• Computerized~~	The Responsible Entity **has not implemented** ~~n~~**or** **has not** **documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	~~Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, 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.~~	~~logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4,~~ ~~**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.~~	~~Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.~~	• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						day, seven days a week.
CIP-006-4c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	N/A~~The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.~~	N/A~~The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.~~	N/A~~The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.~~	~~The Responsible Entity retained physical access logs for less than 45 calendar days.~~ The responsible entity did not retain physical access logs for at least ninety calendar days.
CIP-006-4c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include one of the Requirements R8.1, R8.2, and R8.3.~~	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include two of the Requirements R8.1, R8.2, and R8.3.~~	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include any of the Requirements R8.1, R8.2, and R8.3.~~	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-4c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.2	Retention of testing and	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.				
CIP-006-4c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-007-4	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-007-4, 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.	N/A	N/A	N/A	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-007-4	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.	N/A	N/A	N/A	N/A
CIP-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-4	R2.	Ports and Services — The Responsible Entity shall establish,	N/A	N/A~~The Responsible~~	N/A~~The Responsible~~	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.		~~Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	~~Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	Entity did not establish (implement) ~~n~~or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	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).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R2.3.	In the case where unused ports and services cannot be disabled due to technical	N/A	N/A	N/A	For cases where unused ports and services cannot be

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.				disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk. ~~exposure or state an acceptance of risk.~~
CIP-007-4	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement 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).	N/A~~The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-3 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).~~	N/A~~The Responsible Entity **established (implemented) but did not document**, either separately or as a component of the documented configuration management process specified in CIP-003-3 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).~~	N/A~~The Responsible Entity **documented but did not establish (implement)**, either separately or as a component of the documented configuration management process specified in CIP-003-3 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 (implement)** ~~n~~**or** did not **document**, either separately or as a component of the documented configuration management process specified in CIP-003-4~~3~~ 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).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk. ~~exposure or an acceptance of risk.~~
CIP-007-4	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention	N/A	N/A	N/A	The Responsible Entity, where technically feasible,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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).				did not use anti-virus software or other malicious software (“malware”) prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity **did not document or did not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-4	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	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity did not 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-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented	N/A	N/A	N/A	One or more user

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.				accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
CIP-007-4	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.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4~~3~~ Requirement R5 and Standard CIP-004-~~3~~4 Requirement R4.
CIP-007-4	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		other generic account privileges including factory default accounts.				manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
CIP-007-4	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.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-4	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,	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity has not implemented (one or more components of) a policy for managing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		change in assignment or termination).				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-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-4	R6.	Security Status Monitoring — The Responsible Entity shall ensure that	N/A	N/A	N/A	The Responsible Entity as technically

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				feasible, did not implement automated tools or organizational process controls, to monitor system events that are related to cyber security on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	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.	N/A	N/A	N/A	The Responsible Entity **did not implement or 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.
CIP-007-4	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	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-008-4.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement 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-005-4.	N/A~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic~~	N/A~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security~~	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Security Perimeter(s) as identified and documented in Standard CIP-005-3~~ ~~**but**~~ ~~did not maintain records as specified in R7.3.~~	~~Perimeter(s) as identified and documented in Standard CIP-005- 3~~ ~~**but**~~ ~~did not address redeployment as specified in R7.2.~~	Perimeter(s) as identified and documented in Standard CIP-005-4~~3~~ **but** did not address ~~disposal~~ redeployment as specified in R7.2~~1~~.	Security Perimeter(s) as identified and documented in Standard CIP-005-4~~3~~. 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-005-4 but did not address disposal as specified in R7.1. OR The Responsible Entity did not maintain records pertaining to disposal or[3]

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						redeployment as specified in R7.3.
CIP-007-4	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.	N/A	N/A	N/A	N/A
CIP-007-4	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.	N/A	N/A	N/A	N/A
CIP-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-4	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:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment 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.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-4	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;	N/A	N/A	N/A	N/A
CIP-007-4	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-4	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.	N/A	N/A	N/A	N/A
CIP-007-4	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4~~3~~ at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4~~3~~ at least annually ~~**nor**~~ **and** ~~were~~ changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being completed.
CIP-008-4	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall	N/A	N/A~~The Responsible Entity has developed~~	The Responsible Entity has developed	The Responsible Entity has not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:		~~but not maintained a Cyber Security Incident response plan.~~	a Cyber Security Incident response plan ~~but the plan~~that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with those components. ~~does not address one or more of the subrequirements R1.1 through R1.6.~~	developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6, or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-4	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.	N/A	N/A	N/A	N/A
CIP-008-4	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		changes.				
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-4	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.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-009-4	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:	N/A	N/A	N/A	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 address one or more of the requirements CIP-009-4~~3~~ R1.1 **and** R1.2.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-009-4	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-4	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-4	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-4	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 thirty calendar days of the change being completed.	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 than30 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.~~	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						were not communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty ~~more than 180~~ calendar days of the change.
CIP-009-4	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.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-4	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.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-4	R1.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.	HIGH
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion For the purpose of Standard CIP 002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.	HIGH
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 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	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	
CIP-003-4	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:	MEDIUM
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	LOWER
CIP-003-4	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-003-4	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-4	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-002-4 through CIP-009-4.	~~LOWER~~MEDIUM
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-4	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-4	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).	LOWER
CIP-003-4	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-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOWER
CIP-003-4	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

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-4	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-4	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-002-4, 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.	MEDIUM
CIP-003-4	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-003-4	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-003-4	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-4	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-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	LOWER
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-4	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-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-4	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.	LOWER
CIP-004-4	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets 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:	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		• 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.).	
CIP-004-4	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOWER
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MEDIUM
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-4	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-004-4	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	MEDIUM
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment 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.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-004-4	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-004-4	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-004-4.	LOWER
CIP-004-4	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-004-4	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-004-4	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
CIP-005-4	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-005-4	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).	MEDIUM
CIP-005-4	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.	MEDIUM
CIP-005-4	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).	MEDIUM
CIP-005-4	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-005-4.	MEDIUM
CIP-005-4	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		through R9; Standard CIP-008-4; and Standard CIP-009-4.	
CIP-005-4	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-005-4	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).	MEDIUM
CIP-005-4	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-005-4	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-005-4	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	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.	MEDIUM
CIP-005-4	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-4	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-4	R2.5.2.	The authentication methods.	LOWER
CIP-005-4	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	LOWER
CIP-005-4	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-4	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
CIP-005-4	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.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-4	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.	MEDIUM
CIP-005-4	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.	MEDIUM
CIP-005-4	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:	MEDIUM
CIP-005-4	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-4	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-4	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-4	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	MEDIUM
CIP-005-4	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.	MEDIUM
CIP-005-4	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.	LOWER
CIP-005-4	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.	LOWER
CIP-005-4	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-005-4	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-008-4.	LOWER
CIP-006-4c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-4c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-4c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-4c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	MEDIUM
CIP-006-4c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	MEDIUM
CIP-006-4c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	MEDIUM
CIP-006-4c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	MEDIUM
CIP-006-4c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-4c	R1.8	Annual review of the physical security plan.	LOWER
CIP-006-4c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4a Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	MEDIUM
CIP-006-4c	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		identified Physical Security Perimeter.	
CIP-006-4c	R4	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets	MEDIUM
CIP-006-4c	R5	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-008-4. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-4c	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		selected access control and monitoring method. - Video Recording: Electronic capture of video images of sufficient quality to determine identity. - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	
CIP-006-4c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	LOWER
CIP-006-4c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-4c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-4c	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-4c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-4	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-007-4, 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-007-4	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-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-4	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MEDIUM
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		and emergency operations.	
CIP-007-4	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-007-4	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.	MEDIUM
CIP-007-4	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement 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-007-4	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-007-4	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.	LOWER
CIP-007-4	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).	MEDIUM
CIP-007-4	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.	MEDIUM
CIP-007-4	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.	MEDIUM
CIP-007-4	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-007-4	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.	MEDIUM
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		designated personnel. Refer to Standard CIP-003-4 Requirement R5.	
CIP-007-4	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-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	MEDIUM
CIP-007-4	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-007-4	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.	MEDIUM
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-4	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).	MEDIUM
CIP-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-4	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-007-4	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.	MEDIUM
CIP-007-4	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-4	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-008-4.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement 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-005-4.	LOWER
CIP-007-4	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-007-4	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-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-4	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-007-4	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-4	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;	MEDIUM
CIP-007-4	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-4	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.	MEDIUM
CIP-007-4	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOWER
CIP-008-4	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOWER
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	LOWER
CIP-008-4	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-008-4	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	LOWER
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-4	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
CIP-009-4	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-009-4	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-009-4	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-4	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-009-4	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 thirty calendar days of the change being completed.	LOWER
CIP-009-4	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-009-4	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