Note — This report shows only those VSLs that are associated with requirements that were modified when converting CIP-002-2 through CIP-009-2 into CIP-002-3 through CIP-009-3.

Proposed Violation Severity Levels for the CIP Version 3 Series of Standards (Project 2009-21):

Index:

Standard Number CIP-005-3 — Electronic Security Perimeter(s)				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	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; and Standard CIP-009-3.	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; and Standard CIP-009-3.	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; and Standard CIP-009-3.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-33; 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.

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	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 reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
R1.6. (V3 proposed)	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.	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.	The Responsible Entity did not include or implement a visitor control program in its physical security plan.
R2.	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	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-006-3aRequirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-	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	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

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	CIP-008-3; and Standard CIP-009-3.	3.	CIP-008-3; and Standard CIP-009-3.	Perimeter access point such as electronic lock control mechanisms and badge readers was provided without 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.
R5.	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.	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 nor 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

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**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.	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-008-3.

Standard Number CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R3.	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).	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).	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) nor 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).
R5.1.3.	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.
R7.	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-	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	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 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-

Standard Number CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	005-3 **but** did not maintain records as specified in R7.3.	redeployment as specified in R7.2.	specified in R7.1.	3.
R9.	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 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-007-3 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.