

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Summary Consideration:

The drafting team corrected an error in the Cyber Security VSLs for CIP-003-2 R 2.3 based on balloter comments so that the Severe VSL describes performance that is more noncompliant than the performance for the High VSL. This was the only modification to the VSLs and VRFs for the Cyber Security Standards version 2.

One comment submitted suggests a wording change for a future version of CIP003 R2.4. This comment has been forwarded to the Standards Drafting Team working on Version 4 of the CIP standards.

Most comments submitted with a negative ballot indicated that the VSLs need to account for “risk” and the DT explained that the risk associated with noncompliance is identified by the Violation Risk Factor, not the Violation Severity Level. Violation Severity Levels identify degrees of noncompliant performance without regard to reliability-related risk. Some balloters proposed modifications to the requirements, and this is outside the scope of this project.

In proposing VSLs, the DT gave consideration to the guidelines provided by FERC in its June 19, 2008 Order on Violation Severity Levels:

From: ORDER ON VIOLATION SEVERITY LEVELS PROPOSED BY THE ELECTRIC RELIABILITY ORGANIZATION (Issued June 19, 2008)
17. For purposes of Commission review, and as a useful tool in the future development of new, or revision of current Violation Severity Levels, the Commission has developed four guidelines for evaluating the validity of Violation Severity Level assignments:

- (1) Violation Severity Level assignments should not have the unintended consequence of lowering the current level of compliance;
- (2) Violation Severity Level assignments should ensure uniformity and consistency among all approved Reliability Standards in the determination of penalties;
- (3) Violation Severity Level assignments should be consistent with the corresponding requirement; and
- (4) Violation Severity Level assignments should be based on a single violation, not on a cumulative number of violations. These guidelines will provide a consistent and objective means for assessing, *inter alia*, the consistency, fairness and potential consequences of Violation Severity Level assignments.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.¹

¹ The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
John D. Martinsen	Public Utility District No. 1 of Snohomish County	4	Negative	Although the District reviews the Critical Assets and the list of Critical Cyber Assets on an annual basis, we do not believe the lack of a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list should be considered a Severe VSL. Performing the review and assessment tasks that may uncover reliability exposures is significantly more important than a signature. We believe this is another case where the requirements and exposure to penalties focus on documentation and have little to no impact on regional reliability or reducing the risks of wide-spread cascading outages.
<p>Response: Thank you for your comment. As defined, a VSL is an after the fact look at how well the responsible entity met the intent of the requirement. This is quite different from a violation risk factor which determines (if the requirement were to be violated) what would be the impact to the reliability of the bulk electric system.</p> <p>In assigning VSLs it is assumed that the requirement has been violated and the question that remains is how severely the intent of the requirement has been missed. For example if the requirement states that X must be documented and the responsible entity has not documented X then the intent of the requirement has been missed and therefore the severity level must be severe. Similar conditions apply to any and all requirements that are binary in nature (i.e. the requirement is either met or not met) in that not meeting the requirement can only be a severe violation level. The impact on the BES would be taken care of by the violation risk factor. A documentation type of requirement would likely have a lower risk factor than a requirement for specific action (by the responsible entity) that impacts the BES.</p>				
Richard Kinas	Orlando Utilities Commission	5	Negative	CIP-006 R3 VSL is arbitrarily harsh at a Sever level for "A cyber Asset". Depending on how many assets are used to implement an Entities ESP control system, a miss of a single component that is potnetially composed of dozens of such assets does not seem to match the violation.
<p>Response: Thank you for your comment. Because CIP-006-2 R3 refers to cyber assets used in the access control and/or monitoring of access to the Electronic Security Perimeter. Failure to protect any such cyber asset is considered to be a severe violation due to the potential vulnerability created by such a lack of protection.</p> <p>In assigning VSLs it is assumed that the requirement has been violated and the question that remains is how severely the intent of the requirement has been missed. For example if the requirement states that X must be documented and the responsible entity has not documented X then the intent of the requirement has been missed and therefore the severity level must be severe. Similar conditions apply to any and all requirements that are binary in nature (i.e. the requirement is either met or not met) in that not meeting the requirement can only be a severe violation level. The impact on the BES would be taken care of by the violation risk factor. A documentation type of requirement would likely have a lower risk factor than a requirement for specific action (by the responsible entity) that impacts the BES.</p>				

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Martin Bauer	U.S. Bureau of Reclamation	5	Negative	<p>The CIP-003-2 R 2.3 Violation Level is characterized Severe for what appears to be failure to complete any one of the following requirements through the use of the "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; or changes to the delegated authority are not documented within thirty calendar days of the effective date." This characterization would not be consistent with other Severity Levels which would have been characterized Severe for failure to complete all the requirements.</p> <p>The CIP-003-2 R 2.4 Violation Level is characterized Severe when the senior manager failed to authorize exceptions. The language is ambiguous and can mean of no exceptions used were authorized or documented, or failure to even authorize one exception constitutes a severe violation. There is no allowance for the fact that there may be no exceptions or that no exceptions sought were authorized. The issue can only arise if the exception was implemented and not authorized. Language should read "The senior manager or delegate(s) did not authorize and document as required, one or more exceptions from the requirements of the cyber security policy as required that were invoked or implemented."</p>
<p>Response: Thank you for your comment. You have correctly identified an error in the Severe VSL. The drafting team has changed the word "or" to "and" for the recirculation ballot and will highlight this correction in the announcement for the recirculation ballot.</p> <p>Regarding the comments on CIP-003-2 R2.4, as defined, a VSL is an after the fact look at how well the responsible entity met the intent of the requirement. This is quite different from a violation risk factor which determines (if the requirement were to be violated) what would be the impact to the reliability of the bulk electric system. Further, the drafting team believes the current language, with "as required" at the end, allows for the situation where no exceptions have been sought.</p>				
Carter B Edge	SERC Reliability Corporation	10	Negative	<p>The posting material is so convoluted that I can't understand the specifics of what I am being asked to vote on. Not to mention that the posting indicates that this is an interpretation. If it is an interpretation where is the interpretation request? How is one to know the scope and reasoning for the changes without completely re-working the issue for themselves from version 1 to version 2 of the CIP standards? The drafting team should provide an overview or executive summary of thier work product and approach when asking for approval of such a disparate set of changes.</p>
<p>Response: Thank you for your comment. It appears this comment was meant for another project that was being balloted at the same time as the version 2 CIP standard VSLs.</p>				

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Voter	Entity	Segment	Vote	Comment	
Dana Cabbell	Southern California Edison Co.	1	Affirmative	<p>Although we understand that NERC stakeholders have recently approved a modification to the NERC Reliability Standards Development Procedure that will require that Violation Risk Factors and Violation Severity Levels be developed at the same time and by the same drafting team that drafts the respective underlying reliability standards, we would like you to consider the following recommendations for all future VRF and VSL projects:</p>	
David Schiada		3			<p>1. Concern: There appears to be an inconsistent gradation between reliability standards involving duration-based requirements. Many requirements in the various reliability standards require specific action prior to a defined elapsed time. The VSLs for all reliability standards appear to have inconsistencies when the requirement specifies an action within a defined elapsed time. Recommendation: We recommend enhancing the guideline(s) for VSL development to follow specific criteria for assigning severity level based on elapsed time. The VSLs may be based on some ratio/multiple of the original time stated in the requirement. For example, if a requirement specifies that an action be performed within 30 days, the VSL gradations might use 30 day increments: Lower - Action was performed within 31-60 days Moderate - Action was performed within 61-90 days High - An action was performed within 91-120 days Severe - Either action was not performed or it was performed >120 days.</p>
Marcus V Lotto		6			<p>2. Concern: There appears to be an inconsistency in the use of “binary” VSLs as opposed to “graded” VSLs. Because the decision as to whether a requirement is binary in nature is left to the various VSL drafting teams, it appears to be inconsistently applied. Some requirements that appear amenable to a graded approach have VSLs that are “binary” in nature. Recommendation: We recommend that the development of VSLs occur in conjunction with the development/revision of the respective standard. If the VSLs are developed in conjunction with the requirements, the requirements can be revised as needed to ensure compliance can be measured using the appropriate level. Additionally, we recommend more prescriptive guidance to VSL drafting teams surrounding the use of “binary” VSLs.</p>
				<p>3. Concern: There appears to be an inconsistent use of the “roll up” approach to assigning VSLs. Although the roll-up approach may be beneficial to avoid double jeopardy in some cases, it cannot be utilized in all instances of requirements containing sub-requirements. Since the decision to roll-up is left to the discretion of the various VSL drafting teams, it creates potential inconsistencies. Recommendation: We recommend that the development of VSLs occur in conjunction with the development/revision of the respective reliability standard. If the VSLs are developed in conjunction with the requirements, the requirements can be revised as needed to ensure compliance can be measured using the appropriate</p>	

Consideration of Comments on Initial Ballot — Cyber Security (VRFs and VSLs for Version 2 CIP Standards) (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>level.</p> <p>4. Concern: There appears to be an inconsistent application of percentages in VSLs (i.e. 5% increments in some, but not all). Recommendation: We recommend that the guidelines for development of VSLs include the standardization of percentages, much like the quartiles in the existing VSL Development Guidelines Criteria. Additionally, the development of the VSLs should occur in conjunction with the development/revision of the respective reliability standards. If the VSLs are developed in conjunction with the requirements, the requirements can be revised as needed to ensure compliance can be measured using the appropriate level/gradation. Thank you for your attention to this matter.</p>
<p>Response: Thank you for your comment. The NERC standards development process has been modified to include the development of VSL by the Standards Drafting Team, as documented in the “Drafting Team Guidelines” Endorsed by the SC in its April 2009 revision. The document is available in the Standards Program area web site. NERC filed a proposal for modifying its approach to developing VSLs in August 2009, and this filing does address the issues you identified.</p>				
Guy V. Zito	Northeast Power Coordinating Council, Inc.	10	Affirmative	<p>The severe VSL for CIP003 R2.4 is as follows: The senior manager or delegate(s) did not authorize and document as required, any exceptions from the requirements of the cyber security policy as required. A future revision to the standard should consider a change to “existing” from “any” exceptions. “Any” implies that there must be at least one exception.</p>
<p>Response: Thank you for your comment. This comment will be forwarded to the version 4 CIP standards drafting team for their consideration when developing VSLs for the version 4 cyber security standards.</p>				
Terry Bilke	Midwest ISO, Inc.	2	Abstain	<p>We are turning the ballot over to another person and will cast our official position during recirculation.</p>
<p>Response: Thank you for your comment.</p>				