

Consideration of Comments on Initial Ballot — Cyber Security Violation Severity Levels (Project 2008-14)

Summary Consideration:

The drafting team did not make any modifications to the Cyber Security VSLs based on ballot comments.

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.

Voter	Entity	Segment	Vote	Comment
Kirit S. Shah	Ameren Services	1	Negative	<p>(1) We have concerns that, to a large degree, the violation severity levels (VSLs) do not seem to correspond to actual violation circumstances. For example, many of the VSLs are overly severe for violations that may be simple documentation errors: Under CIP 002, R3: Lack of inclusion of a single critical cyber asset on the list, regardless of whether that asset is effectively protected under the requirements of the standard is a severe VSL under several of the sub-requirements, which is the same as not having a list at all. This type of severity level assignment is inconsistent throughout this document.</p> <p>(2) It is important that the VSL implementation follow the intent of the standards to improve security versus creating documentation. We recommend that the Drafting team evaluate and assign security levels at the requirement level instead of the sub requirement. Since many of the sub-requirements in the standard simply provide more clarification of details within the overall requirement, we suggest that the assessment of severe be reserved for those situations where the top-level requirements are not met at all. Levels lower through higher should be used based upon the severity of non-compliance to the more detailed sub-requirements. For example, is something mis-documented or ignored altogether? These are two very different situations and should be treated as such.</p> <p>(3) A consistent approach needs to be applied to all requirements. The VSLs for some of the standards take a measurable approach with consideration given to severity of the violation, while others are very documentation focused. Other inconsistencies appear in the draft. For example, CIP-003 R6 VSL appears to require 2 processes one for configuration management and one for change control, whereas the standard calls for "a process for change control and configuration management."</p> <p>(4) We believe that these VSLs are not yet ready for practical application within the industry and that significant work is needed on the Violation Severity Levels for the NERC CIP Standards.</p>
Mark Peters		3		
<p>Response: Thank you for your comments. The VSL is a measure of how severely the requirement is violated. If a requirement calls for documentation and the documentation is not done then the requirement is not met. The concern regarding documentation errors compared to whether the asset is protected is a concern about risk. The risk factor for a documentation requirement that does not represent a large adverse impact on reliability is lower than the risk factor for a requirement that calls for the protection of the system and therefore can have a large adverse impact on reliability. Penalties are determined based on both the VRF and VSL for a requirement. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL.</p>				

Voter	Entity	Segment	Vote	Comment
The DT has followed the FERC guidelines and assigned a consistent set of VSLs based on the requirements.				
Richard McLeon	South Texas Electric Cooperative	1	Negative	CIP-002-1 through CIP-009-1 have been replaced making these changes moot. Some of the proposed changes are necessary, but evidence on these reliability standards is now documented under the "unedited" VSL. Any changes of the VSLs should be placed on CIP-002-2 through CIP-009-2 allowing industry to respond accordingly going forward.
Response: Thank you for your comments. The DT is required by the FERC to assign VSLs to all currently approved standards. The revised group of CIP standards has or will be assigned appropriate VSLs and when approved by FERC or other applicable regulatory authorities will replace the current standards. The DT is following the process as required by FERC. The industry has an opportunity to comment and vote on the revised standards including the VSLs.				
Karl E. Kohlrus	City Water, Light & Power of Springfield	5	Affirmative	CIP-005-1 Requirement 5: Using percentages of documentation to determine levels of severity could lead to inconsistent determinations of severity. If documentation doesn't exist, what percentage of the total documentation would it represent? CIP-006-1 Requirement 1.1: The difference between a VSL of High and Severe is subject to interpretation. How do you document a measure that doesn't exist?
Response: Thank you for your comments. If documentation is required and has not been done (does not exist) it would represent zero percent of the total documentation. Percentages can be determined by such things as number of items to be documented. If 20 items are to be documented and one is missing then 5% of the documentation required is missing. While it is recognized that this will require some determination on the part of the compliance enforcement authority, FERC points out that VSLs are a compliance item. VSLs can not always be absolute and some industry members point out that large entities may have thousands of items to document, while smaller entities may have a few. Use of percentages seems to be an equitable way to approach this.				
Raymond Tran	Ascendant Energy Services, LLC	8	Affirmative	Consistency is critical: Use of VSL in standards as well as a basis for penalty and sanction calculation shows consistency. Raymond Tran Director - Power Systems and Compliance Ascendant Energy Services 775-823-9896
Response: Thank you for your comments. The DT has followed the FERC Guidelines in developing the VSLs and consistency in the assignment of VSLs is one of FERC's VSL Guidelines.				
George R. Bartlett	Entergy Corporation	1	Negative	In some cases the severity level does not align with the violation. There are also many undocumented factors that have to be considered before applying a VSL. The VSLs need more industry input before this standard can be approved.
Response: Thank you for your comments. The VSL is a measure of how severely the requirement is violated. You are correct that other factors need to be considered before applying a VSL to determine a penalty or sanction. Specifically the VSL needs to be combined with the Violation Risk Factor (VRF) and considered along with any other aggravating or mitigating factors as identified in the Sanction Guidelines. The				

Voter	Entity	Segment	Vote	Comment
<p>VRF determines the risk associated with each requirement with regards to reliability. Penalties are determined based on both the VRF and the VSL. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL.</p>				
Stephen Ricker	East Kentucky Power Coop.	5	Negative	Many of the VSLs seem to be high for minor issues such as documentation or timing.
<p>Response: Thank you for your comments. The VSL is a measure of how severely the requirement is violated. If a requirement calls for documentation and the documentation is not done then the requirement is not met. The risk factor for a documentation requirement that does not represent a large adverse impact on reliability is lower than the risk factor for a requirement that calls for the protection of the system and therefore can have a large adverse impact on reliability. Penalties are determined based on both the VRF and the VSL for a requirement. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL. The DT has followed the FERC guidelines and assigned a consistent set of VSLs based on the requirements.</p>				
James R. Keller	Wisconsin Electric Power Marketing	3	Negative	<p>Match violation severity level to the impact a missed requirement may have on the BES. To a large degree, the violation severity levels (VSLs) do not seem to correspond to actual violation circumstances. For example, many of the VSLs are overly severe for violations that may be simple documentation errors: Under CIP 002, R3: Lack of inclusion of a single critical cyber asset on the list, regardless of whether that asset is effectively protected under the requirements of the standard is a severe VSL under several of the sub-requirements, which is the same as not having a list at all. This type of severity level assignment is inconsistent throughout this document. In general, severe VSLs should be reserved for more egregious offenses, such as the lack of a program, policy, or procedure altogether or a failure to adequately protect assets, rather than for minor oversights in documentation. The NERC Compliance Training states the following: "A deficient documentation violation would be a less severe violation than a lack of performance violation (lack of training being performed). Documentation violations are less severe than performance violations. A document deficiency versus a performance deficiency is a measure of consideration in the penalty phase." This should consistently be reflected in the VSLs.</p> <p>Apply a consistent approach across all CIP standards. A consistent approach needs to be applied to all requirements. The VSLs for some of the standards take a measurable approach with consideration given to severity of the violation, while others are very documentation focused. More time should be spent working on a</p>
Anthony Jankowski	Wisconsin Energy Corp.	4		
Linda Horn	Wisconsin Electric Power Co.	5		

Voter	Entity	Segment	Vote	Comment
				single consistent approach and applying this approach to all VSL levels. When viewed as a whole, the ratings are inconsistent from one requirement to the next and do not appear to consider the criticality of the item in question. Variations in like-measurements occur throughout. For instance, missing elements for one document will be rated as Moderate, another as Severe, and yet another with a full spectrum based on the percentage of completion. In most cases, the type of document is similar with no significant variance in risk.
<p>Response: Thank you for your comments. The VSL is a measure of how severely the requirement is violated. If a requirement calls for documentation and the documentation is not done then the requirement is not met. The concern regarding documentation errors compared to whether the asset is protected is a concern about risk. The risk factor for a documentation requirement that does not represent a large adverse impact on reliability is lower than the risk factor for a requirement that calls for the protection of the system and therefore can have large adverse impact on reliability. Penalties are determined based on both the VRF and the VSL. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL. The DT has followed the FERC guidelines and assigned a consistent set of VSLs based on the requirements.</p>				
Daniel Duff	Liberty Electric Power LLC	5	Negative	Missing the title of the designated senior manager on paperwork in a file should not be the same severity level as failure to implement a program to protect critical cyber assets.
<p>Response: Thank you for your comments. The VSL is a measure of how severely the requirement is violated. If a requirement calls for documentation and the documentation is not done then the requirement is not met. The concern regarding documentation errors compared to whether the asset is protected is a concern about risk. The risk factor for a documentation requirement that does not represent a large adverse impact on reliability is lower than the risk factor for a requirement that calls for the protection of the system and therefore can have large adverse impact on reliability. Penalties are determined based on both the VRF and the VSL for a requirement. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL. The DT has followed the FERC guidelines and assigned a consistent set of VSLs based on the requirements.</p>				
Richard L. Koch	Nebraska Public Power District	1	Negative	Multiple requirements are treated as "binary" rather than identifying varying levels of non-compliance. For example: CIP-005-1 R1.1, R1.2, R1.3 CIP-007-1 R4.1, R5.1.3, R5.2.2 CIP-009-1 R5
<p>Response: Thank you for your comments. The DT followed the FERC guidelines in developing VSLs. These guidelines state that the language of the VSLs be consistent with the requirement. For those requirements that you point out, the DT believes that the requirements are written such that all of the conditions specified must be met in order for the intent of the requirement to be met. In accordance with the FERC guidelines the DT believes that whenever possible multiple levels of severity are preferable to a single level (as in the binary) however the DT believes that multiple levels are not possible in these requirements.</p>				

Voter	Entity	Segment	Vote	Comment
Edwin Les Barrow	City Public Service of San Antonio	3	Negative	Some of the VSLs seem too high when compared to others. For example, for CIP-003 R2.1, failure to identify business address or title of the senior manager who is otherwise properly designated is a higher VSL than failing to document a change control process. This seems illogical. There are numerous other cases where the levels do not seem to be comparable across various requirements.
<p>Response: Thank you for your comment. Your concern, similar to other industry members, that some VSLs seem to be high for minor issues, is one related to the distinction between VRFs and VSLs. The VSL measures the severity to which the entity has violated (not complied with) the directives of the requirement (not the impact on BES). The VRF measures the impact on reliability (risk) if the requirement is not met. For example, the risk factor for a documentation requirement that does not represent a large adverse impact on reliability will be lower than the risk factor for a requirement that calls for the protection of the system and therefore can have a large adverse impact on reliability. Penalties are determined based on both the VRF and the VSL for a requirement. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL.</p> <p>The DT attempted to be fair and consistent as required by FERC guidelines. This included a significant effort to maintain consistency of the VSLs across requirements. However, this was not possible, or appropriate, in many cases, because some requirements have more elements than others and those elements can vary in their significance in contributing to the intent of the requirement. Consequently the DT felt it appropriate to create violation severity levels to reflect those elements and their significance relative to the requirement (e.g. CIP-003- R6 has documentation, Change Control, and Configuration Management components). Other requirements such as CIP-003 R.2.1 contained fewer significant elements as determined by the DT. As a result there were fewer VSLs, resulting in an appropriate inconsistency between the two requirements.</p>				
David A. Lapinski	Consumers Energy	3	Negative	The assignment of VSLs to the subrequirements (e.g., R1.1) as well as the main requirements (e.g., R1) consistently present the Responsible Entity with a condition of double jeopardy for non-compliance. Almost without exception, the main requirements are written in a fashion as to require that the entity meet the subrequirements as a condition of meeting the main requirement. Therefore, if an entity fails to comply with a subrequirement, even at a fairly low VSL, they will also fail to comply with the main requirement, most of which have only a SEVERE VSL. It's apparent that the eight standards addressed in this ballot were drafted to facilitate VSLs only on the main requirements.
David Frank Ronk		4		
James B Lewis		5		
<p>Response: Thank you for your comments. The DT is aware of the issue of potential double jeopardy. In an attempt to address the concern, the DT rolled up the sub-requirements into the main requirement where possible and assigned VSLs only to the main requirement. The roll up issue is still under discussion with FERC.</p>				

Voter	Entity	Segment	Vote	Comment
Larry Monday	E.ON U.S. LLC	1	Negative	<p>The CIP standards requirements have been the subject of several requests for interpretation. At least one requirement, CIP-006-1a R1.1, has not yet resulted in an approved interpretation from NERC. Many other CIP standard requirements do not properly inform industry as to what should or should not be done in order to avoid penalty. Violation Severity Levels provide a measure as to the degree of non-compliance. Given the ambiguity and confusion of many of the CIP requirements it is difficult to assess the severity of any given means of non-compliance outside that of complete inattention to the standard. For example, many CIP requirements incorporate other standard requirements. In addition to creating confusion, this linkage sets the stage for multiple violations as a result of a single act or omission. Below is a non-exhaustive list of CIP requirements for which compliance is dependent, in whole or in part, upon compliance with other requirements: CIP-003 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: R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations. CIP-005 R1.5 Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009. R2.5.3 The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4. 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. CIP-006 R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009. R5. Access Log Retention “ The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008. CIP-007 R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access</p>
Daryn Barker	Louisville Gas and Electric Co.	6		

Voter	Entity	Segment	Vote	Comment
				privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4. 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. The extent of cross referencing between CIP standard requirements in the requirements listed above and other CIP requirements, and the resulting potential for multiple violations, make it difficult to assess the appropriateness of the VSL assigned to any one such requirement.
<p>Response: Thank you for your comments. The DT is aware of your concerns (also that of others in the industry). The Cyber standards are under revision and the concern of cross-referencing should be raised as part of the standard development process. This drafting team is required to assign VSLs to the existing group of standards based on the existing language and has done so using the FERC guidelines.</p>				
Alan Glazner	Farmington Electric Utility System	1	Negative	The severity levels are unreasonably high compared to the faults. Minor documentation should be treated at a more appropriate level.
<p>Response: Thank you for your comment. Your concern, similar to other industry members, that some VSLs seem to be high for minor issues, is one related to the distinction between VRFs and VSLs. The VSL measures the severity to which the entity has violated (not complied with) the directives of the requirement (not the impact on BES). The VRF measures the impact on reliability (risk) if the requirement is not met. For example, the risk factor for a documentation requirement that does not represent a large adverse impact on reliability will be lower than the risk factor for a requirement that calls for the protection of the system and therefore can have a large adverse impact on reliability. Penalties are determined based on both the VRF and the VSL for a requirement. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL.</p>				
Lee Schuster	Florida Power Corporation	3	Negative	To a large degree, the violation severity levels (VSLs) do not seem to correspond to actual violation circumstances. In many cases the level in the VSLs place more emphasis on documents and record keeping than the cyber security issue at hand. While documents and records are very important, the level of violation noted for many of these instances is not warranted. Progress Energy provided an affirmative vote in the first vote and provided specific references where the VSLs were not properly applied. PGN's notes as submitted in the first vote were not adequately addressed and as such, we vote Negative for the VSLs under consideration.
Wayne Lewis	Progress Energy Carolinas	5		
<p>Response: Thank you for your comment. Your concern, similar to other industry members, that some VSLs seem to be high for minor issues, is one related to the distinction between VRFs and VSLs. The VSL measures the severity to which the entity has violated (not complied with) the directives of the requirement (not the impact on BES). The VRF measures the impact on reliability (risk) if the requirement is not met. For example, the risk factor for a documentation requirement that does not represent a large adverse impact on reliability will be lower than the risk</p>				

Voter	Entity	Segment	Vote	Comment
<p>factor for a requirement that calls for the protection of the system and therefore can have a large adverse impact on reliability. Penalties are determined based on both the VRF and the VSL for a requirement. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL.</p>				
Brad Chase	Orlando Utilities Commission	1	Negative	<p>We have concerns that many issues raised during the open industry comment period have not been resolved in the version being presented for the ballot pool. In addition, the shortened time frame for pre-ballot review may result in insufficient consideration within the industry. Given the importance of these VSLs, we believe that more time should be allotted for industry review and comment and drafting team consideration of these comments. To a large degree, the violation severity levels (VSLs) do not seem to correspond to actual violation circumstances. For example, many of the VSLs are overly severe for violations that may be simple documentation errors: Under CIP 002, R3: Lack of inclusion of a single critical cyber asset on the list, regardless of whether that asset is effectively protected under the requirements of the standard is a severe VSL under several of the sub-requirements, which is the same as not having a list at all. This type of severity level assignment is inconsistent throughout this document. In general, severe VSLs should be reserved for more egregious offenses, such as the lack of a program, policy, or procedure altogether or a failure to adequately protect assets, rather than for minor oversights in documentation. The NERC Compliance Training states the following: "A deficient documentation violation would be a less severe violation than a lack of performance violation (lack of training being performed). Documentation violations are less severe than performance violations. A document deficiency versus a performance deficiency is a measure of consideration in the penalty phase." This should consistently be reflected in the VSLs. We respectfully request that the drafting team re-evaluate the VSLs to allow for a more consistent, measurable basis for severity rather than focusing purely on existence or accuracy of documentation. A review of the matrix shows 118 severe, 75 high, 57 moderate, and 34 lower VSLs. One would think that there should be a more even distribution among the levels. Since many of the sub-requirements in the standard simply provide more clarification of details within the overall requirement, we suggest that the assessment of severe be reserved for those situations where the top-level requirements are not met at all. Levels lower through higher should be used based upon the severity of non-compliance to the more detailed sub-requirements. For example, is something mis-documented or ignored altogether? These are two very different situations and should be treated as such. A</p>
Thomas J. Szelistowski	Tampa Electric Co.	1		
Stanley M Jaskot	Entergy Corporation	5		

Voter	Entity	Segment	Vote	Comment
				<p>consistent approach needs to be applied to all requirements. The VSLs for some of the standards take a measurable approach with consideration given to severity of the violation, while others are very documentation focused. More time should be spent working on a single consistent approach and applying this approach to all VSL levels. When viewed as a whole, the ratings are inconsistent from one requirement to the next and do not appear to consider the criticality of the item in question. Variations in like-measurements occur throughout. For instance, missing elements for one document will be rated as Moderate, another as Severe, and yet another with a full spectrum based on the percentage of completion. In most cases, the type of document is similar with no significant variance in risk. Other inconsistencies appear in the draft. For example, CIP-003 R6 VSL appears to require 2 processes one for configuration management and one for change control, whereas the standard calls for "a process for change control and configuration management." It is important that the VSL implementation follow the intent of the standards to improve security versus creating documentation. We recommend that the Drafting team evaluate and assign security levels at the requirement level instead of the sub requirement. It is our opinion that these VSLs are not yet ready for practical application within the industry. Although we recognize that the FERC/NERC have an aggressive schedule for implementation, we are concerned that the inconsistent treatment of severity levels will result in industry focus on documentation requirements without improving the real security of Critical Cyber Assets and Critical Infrastructure. We believe that significant work is needed on the Violation Severity Levels for the NERC CIP Standards.</p>
Ronald L. Donahey	Tampa Electric Co.	3	Negative	See the comments submitted by T. J. Szelistowski of Tampa Electric Company.
Richard Kinas	Orlando Utilities Commission	5	Negative	OUC agrees with and supports TEC's comments
<p>Response: Thank you for your comments. Regarding your concern that issues raised during the open industry comment period have not been resolved: the drafting team has tried to address all comments received. The shortened timeframe is required in order to meet the FERC schedule for filing the VSLs.</p> <p>Your concern, similar to other industry members, that some VSLs seem to be high for minor issues, is one related to the distinction between VRFs and VSLs. The VSL measures the severity to which the entity has violated (not complied with) the directives of the requirement (not the impact on BES). The VRF measures the impact on reliability (risk) if the requirement is not met. For example, the risk factor for a</p>				

Voter	Entity	Segment	Vote	Comment
<p>documentation requirement that does not represent a large adverse impact on reliability will be lower than the risk factor for a requirement that calls for the protection of the system and therefore can have large adverse impact on reliability. Penalties are determined based on both the VRF and the VSL for a requirement. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL.</p>				
<p>The DT attempted to be fair and consistent as required by FERC guidelines. This included a significant effort to maintain consistency of the VSLs across requirements. However, this was not possible, or appropriate, in many cases, because some requirements have more elements than others and those elements can vary in their significance in contributing to the intent of the requirement. Consequently the DT felt it appropriate to create violation severity levels to reflect those elements and their significance relative to the requirement (e.g. CIP-003- R6 has documentation, Change Control, and Configuration Management components). Other requirements such as CIP-003 R.2.1 contained fewer significant elements as determined by the DT. As a result there were fewer VSLs, resulting in an appropriate inconsistency between the two requirements.</p>				
Terry Bilke	Midwest ISO, Inc.	2	Affirmative	<p>We still are concerned with the approach being taken whereby the VSLs for binary requirements are arbitrarily set to Severe. This causes problems with due process and takes focus from things that really impact reliability. It increases the documentation the Regions must assemble when they use their judgment to temper sanctions for administrative and low risk violations. NERC and the Industry should work together to either more objectively set the VSLs to develop a better approach to handling binary requirements or alternatively provide a separate sanctions matrix for binary requirements.</p>
<p>Response: Thank you for your comments. Where a requirement and the VSL are “binary” in nature, and not conducive to a graded severity level, then a failure to perform the task identified in the requirement can only be classified as “severe”. Your concern, similar to other industry members, that some VSLs seem to be high for minor issues, is one related to the distinction between VRFs and VSLs. The VSL measures the severity to which the entity has violated (not complied with) the directives of the requirement (not the impact on BES). The VRF measures the impact on reliability (risk) if the requirement is not met. For example, the risk factor for a documentation requirement that does not represent a large adverse impact on reliability will be lower than the risk factor for a requirement that calls for the protection of the system and therefore can have a large adverse impact on reliability. Penalties are determined based on both the VRF and the VSL for a requirement. The penalty range for a requirement with a Low VRF and a Severe VSL will be lower than the penalty range for a requirement with a Moderate or High VRF and a Severe VSL.</p>				