

Consideration of Comments on Initial Ballot of Version 1 Risk Factors – Critical Infrastructure Protection

Summary Consideration: While several commenters made suggestions to change one or more of the ratings, there was no consensus to change any one of the ratings, therefore, no changes were made to the violation risk factors for this set of requirements.

Organization:	Baltimore Gas & Electric Company
Member:	John J. Moraski
Comment:	BGE feels that the structure of the voting on risk factors needs to be changed to allow voting on each factor, as opposed to the grouping of the factors as presented. If we disagree with a single factor, we are forced to vote negative on all factors.
Response: Most stakeholders seemed to support the format of the ballot. This comment does not identify any violation risk factor that you feel needs to be modified.	
Organization:	Entergy Corporation
Member:	George R. Bartlett
Comment:	Entergy Transmission believes that several of the VFRs have been rated too high. HIGH should be given to Requirements that directly impact the real-time operations of the bulk electric system. MEDIUM should pertain to those Requirements that prepare an entity for real-time operation, and LOWER for those that are of a reporting nature. The V1 VFRs for the Requirements for which we have concerns were listed in our comments to the ballot pool on 2-9-07. Thank you.
Response: The drafting team reviewed all the comments submitted with the V1 VFRs during the public comment period. The VFRs posted for ballot represented the consensus of stakeholders, based on the ratings selected by stakeholders during the public comment period. There was no consensus to modify the VFRs identified in the comments you submitted.	
Organization:	Minnesota Power, Inc.
Member:	Carol Gerou
Comment:	There were minor inconsistencies with the sub-requirements in the Critical Infrastructure Protection standard set with subrequirements having higher factor than the main requirement. Also, some of the sub-requirements were not rated.
Response: The VFRs posted for ballot represented the consensus of stakeholders, based on the ratings selected by stakeholders during the public comment period. There was an error on the form used to collect stakeholder feedback on the V1 VFRs and insufficient data was collected to develop an accurate VRF for some of the sub-requirements. These VRFs will need to be added when the standards are revised as part of the Three-year Plan for Standards Development.	
Organization:	Sierra Pacific Power Co.
Member:	Richard Salgo
Comment:	Several instances of a sub-Requirement having a higher VRF than it's parent Requirement. Several cases where the sub-requirements are simply a list of options that can be chosen to comply with the main Requirement, yet they still carry a Medium VRF. Some VRF's are missing altogether.
Response: The VFRs posted for ballot represented the consensus of stakeholders, based on the ratings selected by stakeholders during the public comment period. There was an error on the form used to collect stakeholder feedback on the V1 VRFs and insufficient data was collected to develop an accurate VRF for some of the sub-requirements. These VRFs will need to be added when the standards are revised as part of the Three-year Plan for Standards Development.	
Organization:	British Columbia Transmission Corporation

Consideration of Comments on Initial Ballot of Version 1 Risk Factors – Critical Infrastructure Protection

Member:	Phil Park
Comment:	<p>CIP-002-01 – Requirement 2: As CCA's are derived from CA definitions, it would make logical sense that Requirement 2 and 3 would be equally rated. Therefore, it should be considered to increase R2 to Medium.</p> <p>CIP-003-01 – Requirement 5: As information regarding the CCA's will increase a potential attackers intelligence we would consider the access control of that information as CIP-005-01 – Requirement 2: As this is a key control for protection the perimeter, it should be considered to increase the classification to Medium.</p> <p>CIP-005-01 – Requirement 3: Monitoring is a control required to make the perimeter secure. As for physical security monitoring is Medium, a similar reasoning should be considered for the electronic perimeter.</p>
<p>Response: The VRFs posted for ballot represented the consensus of stakeholders, based on the ratings selected by stakeholders during the public comment period. While the drafting team received several suggestions for changes to individual ratings, there was no consensus to change any single rating.</p>	
Organization:	Independent Electricity System Operator
Member:	Don Tench
Comment:	There are significant differences in how we assess the reliability impact of the requirements for cyber security versus the industry survey results. We strongly believe that these requirements should be rated High to Medium.
<p>Response: The VRFs posted for ballot represented the consensus of stakeholders, based on the ratings selected by stakeholders during the public comment period. While the drafting team received several suggestions for changes to individual ratings, there was no consensus to change any single rating.</p>	
Organization:	Midwest ISO, Inc.
Member:	Terry Bilke
Comment:	We want the ERO to be successful and have the tools necessary for a quality compliance program. We agree with the NERC Operating Committee that that the risk factors are weighted too highly. The survey mechanism and current process really are more a measure of perceived importance of the standard than the true risk to the Interconnection. Risk factors were also applied to explanatory text that was never intended to be measured. The standards need to be reformatted to separate the true core requirements from the administrative and explanatory text. Risk factors need to be assigned based on risk of causing cascading failures.
<p>Response: This comment does not identify any violation risk factor that you feel needs to be modified. The violation risk factors will be reviewed in the future as part of the Reliability Standards Development Plan 2007-2009.</p>	
Organization:	Constellation Energy
Member:	Carolyn Ingersoll
Comment:	Upon review of these Version 1 VRF we are voting against their implementation in an effort to highlight that the current method of assigning a VRF to each Requirement and then to each sub requirement, which may be for descriptive purposes only and not contain a specific requirement for a Registered Entity, is not appropriate. For example, INT-004-1 R2 clearly states an action that is required by a Purchasing-Selling Entity and it is appropriate to rate the risk that failure to perform may have on the bulk-power system. However, it is not appropriate to rate the sub-requirements, INT-004-1 R2.1 and R2.2, which are descriptions of how Requirement 2 shall be accomplished by the PSE. There are also numerous Requirements that contain no rating. In addition, we feel that the ratings inappropriately group certain requirements into the Medium or High risk factor

Consideration of Comments on Initial Ballot of Version 1 Risk Factors – Critical Infrastructure Protection

	subgroups, and in light of the fact that the ratings applied to each Requirement cannot be voted on individually we voted against the entire package of standards. In conclusion, we are requesting that the standards drafting team allow participants to vote on individual requirements.
Response: These comments appear to have been entered on the wrong ballot as they duplicate the comments submitted in response to the ballot for Version 1 VRFs for Balance and Interchange.	
Organization:	Xcel Energy, Inc.
Member:	Michael Ibold
Comment:	The Critical Infrastructure standard looks to have been written by IT experts for the operations centers. Unfortunately, it includes the substations and currently there's no easy solution for the substation groups to meet the standard as written. I've talked to other utilities they seem to be headed in one of two directions: 1. Some are having their IT units develop a server/call back system. (Customized programming by each of the utilities.) 2. Others are testing a recently released device from one manufacture that might solve the problem, but is yet untested. The 'technical feasible language' would seem give the utilities an out, but with enough money about any technical challenge can be overcome. So who would decide what is actually 'technically feasible', ..it becomes a bit ambiguous. In addition, a standard in which every utility develops customized programming is not what we should be developing in a 'standard'.
Response: These comments are recommending modifications to the requirements in the Critical Infrastructure standards. This ballot only involves the violation risk factors that were added to the requirements – the drafting team is not authorized to make any changes to the requirements.	
Organization:	Constellation Generation Group
Member:	Michael F. Gildea
Comment:	Upon review of these Version 1 VRF we are voting against their implementation in an effort to highlight that the current method of assigning a VRF to each Requirement and then to each sub requirement, which may be for descriptive purposes only and not contain a specific requirement for a Registered Entity, is not appropriate. For example, CIP-002-1 R3 requires an entity to evaluate their list of Critical Assets and determine if there are any Critical Cyber Assets that are "essential to the operation of the Critical Asset" and is appropriately given a VRF. However, the sub-requirements which are clearly described as the characteristics of a Critical Cyber Asset and are for descriptive purposes should not reflect a VRF. In addition, we feel that the ratings inappropriately group certain requirements into the Medium or High risk factor subgroups, and in light of the fact that the ratings applied to each Requirement cannot be voted on individually we voted against the entire package of standards. In conclusion, we are requesting that the standards drafting team allow participants to vote on individual requirements.
Response: Most stakeholders agreed with the risk factors. The violation risk factors will be reviewed in the future as part of the Reliability Standards Development Plan 2007-2009. Most stakeholders seemed to support the format of the ballot.	
Organization:	Constellation Energy Commodities Group
Member:	Donald Schopp
Comment:	Upon review of these Version 1 VRF we are voting against their implementation in an effort to highlight that the current method of assigning a VRF to each Requirement and then to each sub requirement, which may be for descriptive purposes only and not contain a specific requirement for a Registered Entity, is not appropriate. For example, CIP-002-1 R3 requires an entity to evaluate their list of Critical Assets and determine if there are any Critical Cyber Assets that are "essential to the operation of the Critical Asset" and is appropriately given a VRF. However, the sub-requirements which are clearly described as the characteristics

Consideration of Comments on Initial Ballot of Version 1 Risk Factors – Critical Infrastructure Protection

	<p>of a Critical Cyber Asset and are for descriptive purposes should not reflect a VRF. In addition, we feel that the ratings inappropriately group certain requirements into the Medium or High risk factor subgroups, and in light of the fact that the ratings applied to each Requirement cannot be voted on individually we voted against the entire package of standards. In conclusion, we are requesting that the standards drafting team allow participants to vote on individual requirements.</p>
<p>Response: Most stakeholders agreed with the risk factors. The violation risk factors will be reviewed in the future as part of the Reliability Standards Development Plan 2007-2009. Most stakeholders seemed to support the format of the ballot.</p>	