

Summary Consideration of Comments and Responses to 1st V1 Violation Risk Factors Survey

The Violation Risk Factors Standard Drafting Team thanks all commenters who submitted comments on the second survey of Version 1 violation risk factors. The survey was posted for a 45-day period from July 17–August 30, 2006. The standard drafting team asked stakeholders to complete a survey on the risk factors associated with each requirement in each Version 1 Standard that has been approved or is expected to be approved on or before November 1, 2006. There were 31 surveys submitted, from 78 different people from more than 38 companies representing 6 of the 9 Industry Segments as shown in the table on the following pages.

Based on the ratings and comments received, the drafting team is recommending that the Standards Committee authorize moving the matrix of risk factors forward to ballot with the survey for Version 0 standards.

In the attached ‘Summary Survey’ stakeholder responses have been organized and summarized so that it is easier to see the risk factors selected for each requirement. All surveys received can be viewed in their original format at:

<http://www.nerc.com/~filez/standards/Violation-Risk-Factors.html>

The Version 1 VRF values are the weighted average of the stakeholder VRF selections with changes by the Drafting Team as documented in the attached summary of survey data. For each VRF that was changed, the drafting team provided an explanation of its reasoning for making that change. In most cases, the change was made for one of the following reasons:

- To ensure consistency with the definitions of ‘high, medium, and lower’ risk factors.
- To bring the ratings for sub-requirements into alignment with the rating of the associated requirement.
- To bring consistency to the ratings associated with similar requirements.

If you feel that your comment has been overlooked, 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 Cauley at 609-452-8060 or at gerry.cauley@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.¹

¹ The appeals process is in the Reliability Standards Process Manual:
<http://www.nerc.com/standards/newstandardsprocess.html>.

Summary Consideration of Comments and Responses to 1st V1 Violation Risk Factors Survey

Commenter	Organization	Industry Segment								
		1	2	3	4	5	6	7	8	9
James Sorrels	AEP	x								
Ben Pilleteri	Alabama Power Company			x						
John Sullivan	Ameren									
Doug Johnson	ATC	x								
Phil Parks	BCTC		x							
Dan Taormina	BGE	x								
David Hawkins	CAISO		x							
Gary Brinkworth	City of Tallahassee	x								
Roger McDonald	City of Tallahassee						x			
Rusty Foster	City of Tallahassee			x						
Phil Sobol	Corporate Risk Solutions								x	
Carl Kinsley	Delmarva Power & Light	x								
John Loftis	Dominion	x								
Ernie Scronce	Duke Energy	x								
Sharon Edwards	Duke Energy	x								
Tom Pruitt	Duke Energy	x								
Greg Mason	Dynegy					x				
Ed Davis	Entergy	x								
David Folk	FirstEnergy Corp	x								
Joe Krupar	Florida Municipal Power Agency			x						
Bob Birch	Florida Power & Light	x								
Bob Schoneck	Florida Power & Light	x								
Ed DeVarona	Florida Power & Light	x								
John Shaffer	Florida Power & Light	x								
Eric Senkowicz	FRCC		x							
Linda Campbell	FRCC		x							
Phil Winston	Georgia Power Company			x						
Bill Pope	Gulf Power Company			x						
David Kiguel	Hydro One Networks	x								
Ron Falsetti	IESO		x							
Jim Cyrulewski	ITC	x								
Rebecca Moore	MISO		x							
Joe Stewart	Mississippi Power Company			x						
Denise Roeder	North Carolina Municipal Power Agency			x						
Richard Oswald	Northeast Utilities	x								
Alvin Depew	Pepco	x								

Summary Consideration of Comments and Responses to 1st V1 Violation Risk Factors Survey

Dave Thorne	Pepco	x																	
Mark Godfrey	Pepco Holdings	x																	
Richard Kafka	Pepco Holdings	x																	
Al DiCaprio	PJM		x																
Joe Willson	PJM		x																
Mark Kuras	PJM		x																
Tom Bowe	PJM		x																
Brett Koelsch	Progress Energy	x		x				x	x										
Eric Grant	Progress Energy	x		x				x	x										
Neil Schokey	SCE																		
Andy Bowden	South Carolina Electric & Gas																		
Arnie Cribb	South Carolina Electric & Gas																		
Bob Smith	South Carolina Electric & Gas																		
Brad Stokes	South Carolina Electric & Gas																		
Dan Goldston	South Carolina Electric & Gas																		
Ernie Gibbons	South Carolina Electric & Gas																		
Henry Delk	South Carolina Electric & Gas																		
Hubert Yong	South Carolina Electric & Gas						x												
Jay Hammond	South Carolina Electric & Gas																		
Jerry Lindler	South Carolina Electric & Gas																		
John Blalock	South Carolina Electric & Gas																		
Lee Xanthakos	South Carolina Electric & Gas	x																	
Marion Frick	South Carolina Electric & Gas																		
Oscie Brown	South Carolina Electric & Gas																		
Pat Longshore	South Carolina Electric & Gas																		
Phil Kleckley	South Carolina Electric & Gas																		
Richard Jones	South Carolina Electric & Gas									x									
Sally Wofford	South Carolina Electric & Gas																		
Shawn McCarthy	South Carolina Electric & Gas																		
Simon Shealy	South Carolina Electric & Gas																		
Todd Johnson	South Carolina Electric & Gas																		
Wayne Stuart	South Carolina Electric & Gas																		
Roman Carter	Southern Company	x																	
John Ciza	Southern Company Generation																	x	
Roger Green	Southern Company Generation																	x	
Keith Calhoun	Southern Company Services	x																	
Terry Crawley	Southern Nuclear																		x
Kevin Perry	SPP																		x
Tom Hoffstetter	SPP																		x
Ellis Rankin	TXU Electric Delivery	x																	

Summary Consideration of Comments and Responses to 1st V1 Violation Risk Factors Survey

Travis Besier	TXU Electric Delivery	x											
Nancy Bellows	WAPA												

Summary Consideration of Comments and Responses to 1st V1 Violation Risk Factors Survey

Summary Response to Comments:

These stakeholder comments provide a justification for recommending specific violation risk factor. The drafting team but did not provide individual responses to these comments.

Commenter	CIP	R	Change to	Comment/Reasoning
Sandy Wofford, SCE&G	001		High	CIP-001-1 is not one of the cyber security standards. It deals with reporting sabotage. I would classify violations of the requirements of this standard as "High Risk" because they could potentially put the entire interconnection at risk due to a simple failure to communicate with the appropriate authorities.
Sandy Wofford, SCE&G	002-009		Medium or Low	<p>Based on the definitions in the Risk Factors Comment Form, I would not assign a "High Risk" to any of the violations to the CIP cyber security standards. I may be at odds with the rest of the industry because of the importance placed on cyber security, but the "High Risk" definition states that violations of the requirements would "directly cause or contribute to bulk electric system instability," etc. and I don't think that's the case, although violations would open the door to potential cyber threats.</p> <p>I would assign a "Medium Risk" to all of the violations to the CIP cyber security standards because they "could directly affect the electrical state or capability of the bulk electric system," etc. but they are "unlikely to lead to bulk electric system instability," etc.</p> <p>Furthermore, one could make a case of assigning a "Low Risk" to violations based solely on documentation requirements because they "would not be expected to adversely affect the electrical state or capability of the bulk electric system," etc.</p>
Kevin Perry, Tom Hofstetter; Southwest Power Pool	002-1	3.1	Medium	Critical Cyber Assets (CCAa) are, by definition, among the most sensitive devices. Violating the requirements for protecting such devices meets the criteria for a medium risk because of the potential effect that could result to the bulk electric system.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	003-1	5 5.1 5.1.1 5.1.2 5.2	Lower	The access management program requirements that are described here are administrative in nature, so it would be appropriate to classify them at this level of risk.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	004-1	None listed	Lower	Nothing was marked on the draft; however, this item should be marked as a lower risk requirement since it is administrative in nature.
Kevin Perry, Tom Hofstetter;	004-1	2 2.1 2.2	Medium	Those with hands-on access to CCAs will, by definition, have critical responsibilities. Therefore, their training needs should correspond to the ratings of the assets themselves.

Summary Consideration of Comments and Responses to 1st V1 Violation Risk Factors Survey

Southwest Power Pool		2.2.1 2.2.2 2.2.3 2.2.4		Improper use of critical equipment (i.e., use of CCAs by improperly trained personnel) could quickly negate other security controls.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	004-1	4.2	Medium	If terminated personnel are permitted access to CCAs beyond the listed thresholds, there is significant risk that meets the criteria for a "Medium" ranking.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	005-1	1.1 1.2 1.3	Medium	If an access point to the Electronic Security Perimeter is improperly classified/protected, the risk easily meets the criteria for a "Medium" requirement.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	005-1	1.4 1.5	Medium	In addition to the reasons described in item 6, it's possible that other systems (such as non-critical cyber assets) could be used as a vector for attack of the CCAs; thus, improper protection of those systems should be classified as a "Medium" risk requirement.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	005-1	2 2.1 2.2 2.3 2.4	Medium	By definition, access controls for CCAs are meant to prevent unauthorized access. Thus, the requirements listed here are essential and violations could have an effect that fits this category.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	005-1	4.4	N/A	No change recommended; the draft erred in numbering this requirement.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	006-1	1 1.1 1.2	Medium	Physical security measures need to be properly designed in order to adequately protect CCAs; otherwise, there is a significant increase in risk that warrants the higher ranking.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	006-1	1.6 1.8	Medium	Violation of physical access measures creates the potential for a level of risk that meets the criteria for "Medium"
Kevin Perry, Tom Hofstetter; Southwest Power Pool	006-1	2	Medium	Individually, the sub-categories to this requirement meet the criteria for "Lower"; however, to do nothing would elevate the risk to "Medium" (in effect, the whole is greater than the sum of the parts).
Kevin Perry, Tom Hofstetter; Southwest Power Pool	006-1	3	Medium	Same reasoning as item 12.

Summary Consideration of Comments and Responses to 1st V1 Violation Risk Factors Survey

Kevin Perry, Tom Hofstetter; Southwest Power Pool	007-1	4 4.1	Medium	Failure to use anti-virus tools would pose a risk to CCAs and meet the criteria for a higher ranking than is currently listed.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	007-1	6	Medium	The risks assigned for monitoring the effectiveness of protective measures should be consistent with the value of the CCAs, so the higher ranking is appropriate.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	007-1	7 7.1 7.2	Medium	If assets are not "treated" properly before they are discarded, the risk that residual data could jeopardize the electric system meets the criteria for this level.
Kevin Perry, Tom Hofstetter; Southwest Power Pool	009-1	4	Medium	The fact that data needs to be backed-up indicates its criticality; thus, failure to do so or to test its effectiveness is a logical fit for a medium risk.

Commenter	MOD-024 and MOD-025	R	Change to	Comment/Reasoning
Sandy Wofford, SCE&G				In general, the sharing of system modeling information is vital to overall system reliability. Consequently, setting up standards for how that modeling information is captured and measured is certainly important. However, the two elements of risk associated with these standards don't rise to the level of HIGH risk. First, the risk that the information described in these standards isn't shared in a timely and accurate fashion is low due to recent processes and procedures established in VACAR and SERC to exchange model data in an agreed upon format and in a routine fashion. Second, even if this information were not shared or provided in exactly the fashion outlined in these standards, we probably have enough data from other sources, including real-time SCADA information, to make these standards of low to medium risk.