

The drafting team received several sets of supplementary comments with the surveys for the second draft of the Version 1 Violation Risk Factors. The comments and responses follow:

Supplementary Comments Submitted by Progress Energy:2
Supplementary Comments Submitted by Dominion:.....3
Supplementary Comments Submitted by Entergy Services, Inc:11
Supplementary Comments Submitted by Pepco Holdings, Inc:12
Supplementary Comments Submitted by British Columbia Transmission Company:13

Supplementary Comments Submitted by Progress Energy:

We would like to point out that the survey form had a few problems and would not allow entries for the below identified requirements. Please note the below Progress Energy recommended ratings for these requirements.

- a.. BAL-008-1, R1.3 - LOWER
- b.. CIP-002-1, R3.1 - LOWER
- c.. CIP-003-1, R5.1.2 - LOWER
- d.. CIP 004-1, R2.2.3 - LOWER
- e.. FAC-012-1, R1.2 - LOWER
- f.. FAC-14-1, R5.1.4 – LOWER

[Response: Your selections were used in the final data calculations.](#)

We would also like to point out that the Violation Risk Factors Matrices, for Version 0 and Version 1, were developed using Version 0 of the Vegetation Management Standard (FAC-003-0), which was replaced in early 2006 by FAC-003-1.

The requirements in FAC-003-1, while similar, have been expanded and do not correspond to the requirements and requirement numbering of Version 0. For example, R.2 in FAC-003-0 (VM-Related Outage Reporting) corresponds to R.3 in FAC-003-1, which has been expanded from 2 to 3 VM-related outage categories.

Could NERC please clarify why FAC-003-1 Violation Risk Factors were not included in the Version 1 matrix while the FAC-003-0 Violation Risk Factors were included in the Version 0 matrix?

[Response: The drafting team missed adding the VRFs for FAC-003-1 to the survey for Version 1 Violation Risk Factors.](#)

Supplementary Comments Submitted by Dominion:

BAL-007-1	R2	<p>The Balancing Authority shall maintain a 12-month rolling average of at least 100% on its one-minute Control Performance Measure (CPM).</p> <p>[This is a performance metric as opposed to an administrative requirement. Therefore, it should not have a “Lower” risk factor.]</p>	LOWER	LOWER	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower
BAL-008-1	R2	<p>If there is a Frequency Event and either the FTL is exceeded for more than 30 consecutive clock-minutes or a Frequency Abnormal Limit (FAL) is exceeded for one clock-minute, each Reliability Coordinator within the affected Interconnection shall:</p> <p>[The only requirements here are those listed below in the sub-requirements. Those are all “Medium” risk factors, so there is no reason for R2 to be labeled as “High”.]</p>	HIGH	HIGH	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower
BAL-008-1	R2.1	<p>Notify its Balancing Authorities of the Interconnection frequency conditions.</p> <p>[See comment on R2 above.]</p>	MEDIUM	MEDIUM	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower

Supplementary Comments Submitted with 2nd Survey of V1 Violation Risk Factors

BAL-008-1	R2.2	Direct each of its Balancing Authorities with an ACE in the same direction as the Frequency Error to act to return ACE to zero. [See comment on R2 above.]	MEDIUM	MEDIUM	<input type="radio"/> High <input checked="" type="radio"/> Medium <input type="radio"/> Lower
BAL-008-1	R2.3	Notify its Balancing Authorities when the Interconnection frequency has returned to a value that is within the FTLs. [See comment on R2 above.]	MEDIUM	MEDIUM	<input type="radio"/> High <input checked="" type="radio"/> Medium <input type="radio"/> Lower
CIP-002-1	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	MEDIUM	MEDIUM	<input type="radio"/> High <input checked="" type="radio"/> Medium <input type="radio"/> Lower [This requirement and its sub-requirements are administrative in nature and are subject to only an annual review.]

Supplementary Comments Submitted with 2nd Survey of V1 Violation Risk Factors

CIP-002-1	R3.1.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, [See comment on R3 above.]	MEDIUM	MEDIUM	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Lower
CIP-002-1	R3.2.	The Cyber Asset uses a routable protocol within a control center; or, [See comment on R3 above.]	MEDIUM	MEDIUM	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Lower
CIP-002-1	R3.3.	The Cyber Asset is dial-up accessible. [If sub-requirements R3.1 and R3.2 are ultimately judged to be “Medium” risk factors, then so should this one be.]	LOWER	LOWER	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Lower
CIP-006-1	R3.	Monitoring Physical Access — The Responsible Entity shall document and implement 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. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used: [I read this requirement to say that you must comply with at least one of the following sub-requirements, but you	MEDIUM	MEDIUM	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower

Supplementary Comments Submitted with 2nd Survey of V1 Violation Risk Factors

		don't have to comply with both. They should both have the same risk factor – "Medium".]			
CIP-006-1	R3.1.	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. [See comment on R3 above.]	MEDIUM	MEDIUM	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower
CIP-006-1	R3.2.	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3. [See comment on R3 above.]	LOWER	LOWER	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower
CIP-007-1	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following: [This should have a "Medium" risk factor to be consistent with the risk factors assigned to the annual review of the physical security plan in CIP-006 and the annual cyber vulnerability assessment of electronic access points in CIP-005.]	LOWER	LOWER	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower

Supplementary Comments Submitted with 2nd Survey of V1 Violation Risk Factors

IRO-014-1	R1.1.5.	<p>Coordination of information exchange to support reliability assessments.</p> <p>[Not meeting this requirement means that the RC-to-RC procedures do not address the issue. This rises to the level of “Medium” risk factor to be consistent with the “Medium” ranking of other sub-requirements that identify what must be included in such procedures. The other sub-requirements include outage coordination, reactive resource coordination, capacity shortages, etc.]</p>	LOWER	0	<input type="radio"/> High <input checked="" type="radio"/> Medium <input type="radio"/> Lower
IRO-014-1	R1.1.6.	<p>Authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas.</p> <p>[Not meeting this requirement means that the RC-to-RC procedures do not address the issue. This rises to the level of “Medium” risk factor to be consistent with the “Medium” ranking of other sub-requirements that identify what must be included in such procedures. The other sub-requirements include outage coordination, reactive resource coordination, capacity shortages, etc.]</p>	LOWER	LOWER	<input type="radio"/> High <input checked="" type="radio"/> Medium <input type="radio"/> Lower
IRO-015-1	R1.	<p>The Reliability Coordinator shall follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators.</p> <p>[See comment on R1.1 below.]</p>	MEDIUM	HIGH	<input type="radio"/> High <input type="radio"/> Medium <input type="radio"/> Lower

Supplementary Comments Submitted with 2nd Survey of V1 Violation Risk Factors

IRO-016-1	R1.2.	<p>If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).</p> <p>[See comment on R1 above.]</p>	HIGH	HIGH	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower
IRO-016-1	R1.2.1.	<p>If time permits, this re-evaluation shall be done before taking corrective actions.</p> <p>[See comment on R1 above.]</p>	HIGH	MEDIUM	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower
IRO-016-1	R1.2.2.	<p>If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.</p> <p>[See comment on R1 above.]</p>	HIGH	HIGH	
IRO-016-1	R1.3.	<p>If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.</p> <p>[See comment on R1 above.]</p>	HIGH	HIGH	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower

Supplementary Comments Submitted with 2nd Survey of V1 Violation Risk Factors

IRO-016-1	R2.	<p>The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.</p> <p>[This seems like an after-the-fact administrative process.]</p>	MEDIUM	MEDIUM	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Lower
VAR-001-1	R11	<p>After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.</p> <p>[If this documentation is what enables the implementation, then the risk factor should be "Medium".]</p>	LOWER	LOWER	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower
VAR-001-1	R3.1	<p>Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.</p> <p>[If this list is what informs the operators that these units cannot be depended upon to regulate voltage, then the risk factor should be "Medium".]</p>	LOWER	LOWER	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Lower

Response: The industry determined the VRFs for the Standards/requirements by majority vote. There are not enough comments on the standards you reference to override the industry's VRF values.

Supplementary Comments Submitted by Entergy Services, Inc:

In general, why is there a need to assign a VRF to a phrase that has no actual requirement? Specifically I am referring to those 'requirements' that state, "An entity shall:" with the actual requirements listed below.

Examples: BAL-008-1 R2 is not a requirement and therefore should not have a VRF associated with it. BAL-008-01 R2.1 and 2.2 are requirements and have VRFs.

There is no need to assign VRFs to "R" items with no actual requirement.

Changes to Standards will be addressed by the NERC Reliability Standards Development Plan: 2007-2009 which will review and revise as necessary all reliability standards. Please refer to the posted work plan for details.

Supplementary Comments Submitted by Pepco Holdings, Inc:

CIP-002-1, R3.3

This requirement is equivalent to CIP-005-1, R1.2 which the SDT has rated MEDIUM

CIP-003-1, R4.3

The requirement to implement an action plan to remediate deficiencies raises this to a MEDIUM Risk Factor

FAC-010-1, R2.4

This requirement is almost the definition of HIGH VRF

FAC-011-1, R1

This VRF should be equivalent to that for FAC-010-1 (MEDIUM)

Response: The industry determined the VRFs for the standards/requirements by majority vote. There are not enough comments on the standards/requirements you reference to override the industry's VRF values.

Supplementary Comments Submitted by British Columbia Transmission Company:

<u>Standard Requirement</u>	<u>NERC VRF</u>	<u>BCTC VRF</u>	<u>Explanation of BCTC VRF</u>
FAC-010-1 R1	Medium	Lower	This requirement, in the context of other Requirements, only adds documentation of the Methodology. This is an administrative Requirement.
FAC-010-1 R2 (including R2.1 to R2.5.1)	Medium	High	This is the fundamental Requirement for Planning Authorities to determine SOLs according performance standards. If SOLs are not determined in accordance with performance standards, operators will not have the information necessary to monitor for SOL violations (Ref. IRO-002, 3, 4). This could directly contribute to widespread outage should a contingency occur. The VRF for FAC-010-1 R2 should be the same as IRO - 001, 3, 4.
FAC-011-1 R1	Medium	Lower	This requirement, in the context of other Requirements, only adds documentation of the Methodology. This is an administrative Requirement.
FAC-011-1 R2 (including R2.1 to R2.4)	Medium	High	This is the fundamental Requirement for Reliability Coordinators to determine SOLs according performance standards. As for FAC-010-1, if SOLs are not determined in accordance with performance standards, this could directly contribute to widespread outage should a contingency occur. Determination of SOLs should have the same VRF as the use of SOLs.
FAC-013-1 R1	Medium	High	Same as for SOLs, if Transfer Capabilities are not determined, operators will not have reliable information necessary to monitor violations. This could directly contribute to widespread outage should a contingency occur.
FAC-013-1 R2 to R2.2	Medium	High	If Transfer Capabilities are not communicated, operators and Reliability Coordinators will not have reliable information necessary to monitor violations. This could directly contribute to widespread outage should a contingency occur.
FAC-014-1 R1	Medium	High	If SOLs and IROLs are not established, operators and Reliability Coordinators will not have reliable information necessary to monitor violations. This could directly contribute to widespread outage should a contingency occur.
FAC-014-1 R2	Medium	High	If SOLs and IROLs are not established, operators and Reliability Coordinators will not have reliable information necessary to monitor violations. This could directly contribute to widespread outage should a contingency occur.

Supplementary Comments Submitted with 2nd Survey of V1 Violation Risk Factors

FAC-014-1 R3	Medium	High	If SOLs and IROLs are not established consistent with the SOL methodology, operators and Reliability Coordinators will not have reliable information necessary to monitor violations. This could directly contribute to widespread outage should a contingency occur.
FAC-014-1 R4	Medium	High	These are the SOLs to be provided under FAC-014-1 R5. If SOLs and IROLs are not established consistent with the SOL methodology, operators and Reliability Coordinators will not have reliable information necessary to monitor violations. This could directly contribute to widespread outage should a contingency occur.
FAC-014-1 R5 to R5.4	Medium	High	If SOLs and IROLs are not communicated, entities with a reliability based need will not have information necessary to ensure reliability. This could directly contribute to widespread outage should a contingency occur.
FAC-014-1 R6 to R6.1	Medium	High	Without the stability limits of credible multiple contingencies known to RC, the system could be operated unsafely and resulting in instability and potential collapse should the contingency occur.
IRO-014-1 R1.1.6	Medium	High	Reliability Coordinators are the interface with other Reliability Coordinators. Lack of authority to act in this role can directly contribute to widespread outage.
IRO-015-1 R1.1	Medium	High	Reliability Coordinators are the interface with other Reliability Coordinators. Notifications not given can directly contribute to widespread outage.
IRO-015-1 R3	Medium	High	Reliability Coordinators are the interface with other Reliability Coordinators. If information is not provided, this can directly contribute to widespread outage.

Response: The industry determined the VRFs for the Standards/requirements by majority vote. There are not enough comments on the standards/requirements you reference to override the industry's VRF value(s).