



Debra A. Palmer  
202-778-6439  
dpalmer@schiffhardin.com

1666 K STREET N.W., SUITE 300  
WASHINGTON, DC 20006

t 202.778.6400  
f 202.778.6460

www.schiffhardin.com

March 23, 2007

**VIA ELECTRONIC FILING**

Ms. Magalie R. Salas  
Secretary  
Federal Energy Regulatory Commission  
888 First Street, N.E.  
Washington, D.C. 20426

Re: *North American Electric Reliability Corporation, Docket No. RR07-\_\_\_\_-000*

Dear Ms. Salas:

The North American Electric Reliability Corporation (“NERC”) hereby submits to the Commission for approval the proposed violation risk factors for requirements in NERC’s Version 1 reliability standards included in the NERC reliability standards approved by the Commission in its Order No. 693 issued March 16, 2007. This filing also submits violation risk factors for additional Version 1 reliability standards that are pending approval in Docket RM06-16 or in other dockets. NERC also notes that on February 23, 2007, it filed proposed Version 0 violation risk factors for approval by the Commission, which are under consideration in Docket RR07-9.

Please contact the undersigned if you have any questions.

Respectfully submitted,

/s/ Debra A. Palmer  
Owen E. MacBride  
Debra Ann Palmer

*Attorneys for  
North American Electric Reliability  
Corporation*

Enclosures



## TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	NOTICES AND COMMUNICATIONS	2
III.	BACKGROUND ON DEVELOPMENT OF VIOLATION RISK FACTORS	2
IV.	OVERVIEW OF THE PROPOSED VIOLATION RISK FACTORS	8
	Table 1	10
V.	CONCLUSION	11

EXHIBIT A – PROPOSED VIOLATION RISK FACTORS FOR VERSION 1  
RELIABILITY STANDARDS

EXHIBIT B – RECORD OF DEVELOPMENT (Provided separately)

EXHIBIT C – STANDARDS DRAFTING TEAM ROSTER

EXHIBIT D – FEDERAL REGISTER NOTICE

## I. INTRODUCTION

The North American Electric Reliability Corporation (“NERC”)<sup>1</sup> hereby submits to the Commission for approval the proposed Version 1 violation risk factors for the associated requirements in Version 1 reliability standards<sup>2</sup> that are contained in the 83 reliability standards the Commission approved in Order No. 693.<sup>3</sup> With the exceptions noted below, this filing represents the final set of proposed violation risk factors for all reliability standards that the Commission has approved as mandatory and enforceable in Order No. 693. This filing also contains violation risk factors for proposed standards that the Commission has said in Order No. 693 will remain pending at the Commission until further information is provided or that are pending in another docket at the Commission.

A violation risk factor has been assigned to each requirement of the Version 1 reliability standards to delineate the relative risk to the bulk power system associated with the violation of each requirement. The violation risk factors alone do not change the meaning or intent of the standards. The violation risk factors will be used by NERC and the regional entities in determining financial penalties for violating the standards, as described in Section 4 of the *ERO Sanction Guidelines*, Appendix 4B to the NERC Rules of Procedure.

With respect to the standards the Commission approved in Order No. 693, NERC has not yet developed violation risk factors for any of the requirements for FAC-003-1 or for one

---

<sup>1</sup> NERC has been certified by the Commission as the electric reliability organization (“ERO”) authorized by Section 215 of the Federal Power Act. The Commission certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000. 116 FERC ¶ 61,062 (2006).

<sup>2</sup> Although nominally referred to as “Version 1” risk factors and “Version 1” reliability standards as a short-hand convenience, NERC observes that certain of the standards and associated violation risk factors carry a “-2” designation.

<sup>3</sup> Order No. 693, Mandatory Reliability Standards for the Bulk Power System, 118 FERC ¶ 61,218 (issued Mar. 16, 2007).

requirement each in COM-002-2 and PRC-005-1, as detailed further in Section III of this filing. NERC commits to developing these violation risk factors for filing with the Commission by May 4, 2007. See Section III of this filing, below.

**Table 1** below lists the reliability standards for which violation risk factors are being submitted in this filing. **Exhibit A** to this filing presents the violation risk factors that have been assigned to each requirement in the relevant reliability standards. **Exhibit B** (provided separately from this document due to its volume) presents the record of development of the violation risk factors. **Exhibit C** provides the roster of the drafting team that developed, with the stakeholders, the violation risk factors. **Exhibit D** provides a notice for the *Federal Register*.

## **II. NOTICES AND COMMUNICATIONS**

Notices and communications with respect to this filing may be addressed to the following:

Rick Sergel  
President and Chief Executive Officer  
David N. Cook\*  
Vice President and General Counsel  
North American Electric Reliability  
Corporation  
116-390 Village Boulevard  
Princeton, NJ 08540-5721  
(609) 452-8060  
(609) 452-9550 – facsimile  
[rick.sergel@nerc.net](mailto:rick.sergel@nerc.net)  
[david.cook@nerc.net](mailto:david.cook@nerc.net)

Owen E. MacBride  
Debra Ann Palmer\*  
Schiff Hardin LLP  
1666 K Street, N.W.  
Suite 300  
Washington, DC 20006  
(202) 778-6400  
(202) 778-6460 – facsimile  
[omacbride@schiffhardin.com](mailto:omacbride@schiffhardin.com)  
[dpalmer@schiffhardin.com](mailto:dpalmer@schiffhardin.com)

\*Persons to be included on the Commission's service list are indicated with an asterisk.

## **III. BACKGROUND ON DEVELOPMENT OF VIOLATION RISK FACTORS**

The concept of violation risk factors was originally envisioned by the NERC Board of Trustees several years ago as a way to rank the relative importance of standards violations. In 2004, the NERC Compliance and Certification Committee implemented a reporting process that

included a plan to refine the descriptions of violations that were to be reported to the NERC Board of Trustees and determine if the violations were significant. In February 2005, the Board asked the NERC Compliance and Certification Committee and the Compliance and Certification Managers Committee to complete the process for classifying compliance violations, so that the Board and the public could better understand the significance of each violation.

In October 2005, the NERC Standards Committee and the Compliance and Certification Committee agreed to a set of definitions and to an approach to develop the violation risk factors within the standards development process. In January 2006, the Enforcement, Sanctions, and Disclosure Subcommittee of the Compliance and Certification Committee submitted a standards authorization request (“SAR”) to develop the risk factors. The SAR is the foundational document used in the NERC standards development process to request a new standard or the revision of an existing standard. The SAR and a preliminary list of violation risk factors for the Version 0 reliability standards were posted for public comment in February 2006. Once the SAR was authorized by the Standards Committee for development, the drafting team surveyed the industry twice to gather input and feedback on the proposed violation risk factors. The initial survey was conducted from April 2006 to June 2006, and the second survey was conducted from July 2006 to August 2006. The drafting team made adjustments to the Version 0 violation risk factors to reflect the consensus of the industry.

As the violation risk factors were being developed, NERC proposed in its application for certification as the ERO (filed April 4, 2006) that the violation risk factors should be used for

compliance enforcement as an initial element in the setting of financial penalties, as described in the *ERO Sanction Guidelines* submitted with that application.<sup>4</sup>

Subsequently, the Standards Committee tasked the violation risk factor drafting team with adding violation risk factors to all new and revised reliability standards that the team anticipated would be completed and filed for approval through November 2006, to ensure that all standards approved for implementation by June 2007 would have associated violation risk factors. The resulting violation risk factors for the Version 1 reliability standards were subject to a single round of public comment from July 2006 to August 2006.

The combined table of Version 0 and Version 1 violation risk factors was then put to a vote of stakeholders from October 6 to October 16, 2006. The weighted average vote of the ballot pool was 54% in the affirmative, which fell short of the required two-thirds weighted average affirmative vote required for approval.<sup>5</sup> The ballot was terminated and the violation risk factors were not approved. However, stakeholder comments received during the ballot had revealed a strong desire to separate the Version 0 and Version 1 risk factors, to allow a second round of public comment on the Version 1 risk factors, and to further subdivide the Version 0 risk factors into related “family” groupings of standards for balloting purposes.

As a result, the Version 0 violation risk factors were divided into nine groups of related reliability standards. The Version 0 violation risk factors were then balloted on December 4-5,

---

<sup>4</sup> See *Request of the North American Electric Reliability Council and North American Electric Reliability Corporation for Certification as the Electric Reliability Organization*, Docket RR06-1-000 (April 4, 2006), at 64-65.

<sup>5</sup> Under the NERC Reliability Standards Development Procedure, approval of a new or revised reliability standard requires a quorum of 75% of the members of the registered ballot pool for the proposed standard, and a two-thirds affirmative majority of the weighted segment votes cast. The number of votes cast is the sum of the affirmative and negative votes, excluding abstentions and non-responses.

2006, and, after careful consideration of comments from the initial ballot, re-balloted from February 2 to February 11, 2007. The second ballot resulted in stakeholder approval of the Version 0 violation risk factors. The Version 0 violation risk factors were approved by the NERC Board of Trustees February 13, 2007, and filed for Commission approval February 23, 2007.<sup>6</sup>

A second round of public comment was conducted on the Version 1 violation risk factors from November 2 to December 1, 2006. After incorporation of comments, an initial ballot for the seven groups of Version 1 risk factors was held from February 14 to February 23, 2007. A second ballot was held from February 28 to March 9, 2007. The balloting resulted in approval of all the violation risk factors for the Version 1 reliability standards. The results of the final stakeholder ballot for the violation risk factors for the Version 1 reliability standards were as follows:

Version 1 Violation Risk Factor Group	Quorum Percentage	Weighted Segment Vote
Critical Infrastructure Protection	83%	88%
Facility Ratings	85%	86%
Balancing and Interchange	84%	94%
Interconnection Reliability Operations	82%	86%
Modeling	84%	90%
Protection & Control	85%	93%
Emergency Operations, Voltage Control, and Transmission Operations	83%	86%

The NERC board approved the Version 1 violation risk factors on March 12, 2007.

---

<sup>6</sup> Request of the North American Electric Reliability Corporation for Approval of Violation Risk Factors for Version 0 Reliability Standards, filed February 23, 2007 (Docket No. RR07-9-000).

Accordingly, this filing presents for Commission approval violation risk factors for the Version 1 reliability standards. With the submission for approval of the violation risk factors for the Version 1 reliability standards, every requirement in the 83 NERC reliability standards approved by the Commission in Order No. 693 has an assigned violation risk factor, with the few exceptions noted below. Approval of the violation risk factors submitted in this filing will give the ERO and the regional entities the ability to enforce compliance with reliability standards that have been approved by the Commission in Order No. 693.

Each violation risk factor assignment will be included for review as part of NERC's required five-year review of each reliability standard, or is already included in NERC's three-year standards development work plan.<sup>7</sup>

As it prepared this filing, NERC performed a comprehensive review of its reliability standards pending for approval by the Commission (including those that have now been approved in Order No. 693) to identify any omissions in violation risk factor assignment. Upon review of the nearly 1,300 requirements included in the standards submitted to the Commission for approval, NERC identified six individual requirements without an assigned violation risk factor:

- COM-002-2 Requirement R2
- FAC-010-1 Requirement R2.3.2
- FAC-014-1 Requirement R6.2
- PRC-003-1 Requirement R3
- PRC-005-1 Requirement R2.1
- PRC-014-0 Requirement R3.5

---

<sup>7</sup> See Informational Filing on the North American Electric Reliability Council's and North American Electric Reliability Corporation's Reliability Standards Development Plan: 2007–2009, filed December 1, 2006 in Docket No. RM06-16.

In addition, NERC identified that reliability standards PRC-020-1 and FAC-003-1 did not have violation risk factors assigned for any requirements. Of these eight reliability standards, COM-002-2, PRC-005-1 and FAC-003-1 are included in the reliability standards the Commission approved in Order No. 693. To ensure NERC is prepared to enforce mandatory compliance with these Commission-approved reliability standards beginning in June 2007, NERC will employ its urgent action standards development process to assign violation risk factors to these standard requirements and will file the resulting violation risk factors for Commission approval by May 4, 2007.<sup>8</sup> With that filing, NERC will have developed and submitted for Commission approval violation risk factors for each requirement of the 83 reliability standards approved by the Commission in Order No. 693.

In Order No. 693, the Commission designated reliability standards PRC-003-1, PRC-014-0, and PRC-020-1 in the category of “pending” until NERC provides further information and/or modifications. Violation risk factors for these standards will be addressed through the routine standards development process and filed with the Commission for approval as soon as they are available.

Reliability standards FAC-010-1 and FAC-014-1 are pending Commission approval in Docket No. RM07-3-000. Thus, these standards are not included in the 83 standards approved in Order No. 693. To be prepared for Commission action on these standards should they be approved, violation risk factors for these standards are also included in the urgent action process previously referenced, and will be filed for approval with the Commission by May 4, 2007.

---

<sup>8</sup> NERC’s Standards Committee has authorized the urgent action process for the assignment of the required violation risk factors, and NERC has posted the proposed violation risk factors for a 30-day pre-ballot review.

#### IV. OVERVIEW OF THE PROPOSED VIOLATION RISK FACTORS

Section 4.1.1 of the *ERO Sanction Guidelines* states that NERC will assign a risk factor of “high”, “medium”, or “lower” to each requirement in a NERC reliability standard. In accordance with this the *ERO Sanction Guidelines*, the violation risk factors associated with reliability standards requirements are placed into one of the following three risk categories:

- **High Risk Requirement** — (a) Is a requirement that, if violated, could directly cause or contribute to bulk power system instability, separation, or a cascading sequence of failures, or could place the bulk power system at an unacceptable risk of instability, separation, or cascading failures; or (b) is a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk power system instability, separation, or a cascading sequence of failures, or could place the bulk power system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.
- **Medium Risk Requirement** — (a) Is a requirement that, if violated, could directly affect the electrical state or the capability of the bulk power system, or the ability to effectively monitor and control the bulk power system, but is unlikely to lead to bulk power system instability, separation, or cascading failures; or (b) is a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly affect the electrical state or capability of the bulk power system, or the ability to effectively monitor, control, or restore the bulk power system, but is unlikely, under emergency, abnormal, or restoration conditions anticipated

by the preparations, to lead to bulk power system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

- **Lower Risk Requirement** — Is administrative in nature and (a) is a requirement that, if violated, would not be expected to affect the electrical state or capability of the bulk power system, or the ability to effectively monitor and control the bulk power system; or (b) is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to affect the electrical state or capability of the bulk power system, or the ability to effectively monitor, control, or restore the bulk power system.

Violation risk factors represent one element that will be used by NERC and regional entities to determine monetary and non-monetary penalties when a requirement of a reliability standard has been violated. Violation severity levels – lower, moderate, high, and severe – measure the degree to which a requirement was violated. The violation risk factors, coupled with violation severity levels, set the range for the base penalty amount for a violation of a specific requirement.<sup>9</sup> The violation risk factors represent a key element of the NERC reliability standards and the compliance and enforcement process. The violation risk factors are a determinant of the base range of penalties for violations of requirements in reliability standards, in accordance with the NERC Rules of Procedure.

---

<sup>9</sup> Appendix A of the *ERO Sanction Guidelines* provides a table illustrating the use of violation risk factors in determining penalties.

**Table 1 — Version 1 Violation Risk Factor Submission – Affected Standards**

Status code: 1 = Standard approved in Order No. 693 for which NERC is submitting VRFs.  
 2 = Standard designated as “pending” in Order No. 693 for which NERC is submitting VRFs.  
 3 = Standard pending in another docket for which NERC is submitting VRFs.

Number	Title	Status
BAL-006-1	Inadvertent Interchange	1
CIP-002-1	Critical Cyber Asset Identification	3
CIP-003-1	Security Management Controls	3
CIP-004-1	Personnel and Training	3
CIP-005-1	Electronic Security Perimeters	3
CIP-006-1	Physical Security of Critical Cyber Assets	3
CIP-007-1	Systems Security Management	3
CIP-008-1	Incident Reporting and Response Planning	3
CIP-009-1	Recovery Plans for Critical Cyber Assets	3
EOP-005-1	System Restoration Plans	1
FAC-008-1	Facility Ratings Methodology	1
FAC-009-1	Establish and Communicate Facility Ratings	1
FAC-010-1	System Operating Limits Methodology for the Planning Horizon	3
FAC-011-1	System Operating Limits Methodology for the Operations Horizon	3
FAC-012-1	Transfer Capability Methodology	2
FAC-013-1	Establish and Communicate Transfer Capabilities	1
FAC-014-1	Establish and Communicate System Operating Limits	3
INT-001-2	Interchange Information	1
INT-003-2	Interchange Transaction Implementation	1
INT-004-1	Dynamic Interchange Transaction Modifications	1
INT-005-1	Interchange Authority Distributes Arranged Interchange	1
INT-006-1	Response to Interchange Authority	1
INT-007-1	Interchange Confirmation	1
INT-008-1	Interchange Authority Distributes Status	1
INT-009-1	Implementation of Interchange	1
INT-010-1	Interchange Coordination Exceptions	1
IRO-014-1	Procedures, Processes or Plans to Support Coordination Between Reliability Coordinators	1
IRO-015-1	Notifications and Information Exchange Between Reliability Coordinators	1
IRO-016-1	Coordination of Real-time Activities Between Reliability Coordinators	1
MOD-013-1	Maintenance and Distribution of Dynamics Data Requirements and Reporting Procedures	2
MOD-016-1	Documentation of Data Reporting Requirements for Actual and Forecast	1

Number	Title	Status
	Demands, Net Energy for Load, and Controllable DSM	
MOD-024-1	Verification of Generator Gross and Net Real Power Capability	2
MOD-025-1	Verification of Generator Gross and Net Reactive Power Capability	2
PRC-002-1	Define and Document Disturbance Monitoring Equipment Requirements	2
PRC-018-1	Disturbance Monitoring Equipment Installation and Data Reporting	1
PRC-021-1	Under-Voltage Load Shedding Program Data	1
PRC-022-1	Under-Voltage Load Shedding Program Performance	1
TOP-002-2	Normal Operations Planning	1
VAR-001-1	Voltage and Reactive Control	1
VAR-002-1	Generator Operation for Maintaining Network Voltage Schedules	1

## V. CONCLUSION

NERC respectfully requests that the Commission approve the proposed violation risk factors that are being submitted with this filing for standards that the Commission approved in Order No. 693 (marked as “Status Code 1” on **Table 1**) in sufficient time the violation risk factors will be available for use at the time the reliability standards approved in Order No. 693 become effective. NERC requests that the Commission approve the remaining violation risk factors submitted with this filing (marked as “Status Code 2” and “Status Code 3” on **Table 1**) at such time as the Commission takes action on the related reliability standards.

Respectfully submitted,

/s/ Rick Sergel  
 President and Chief Executive Officer  
 David N. Cook  
 Vice President and General Counsel  
 North American Electric Reliability Corporation  
 116-390 Village Boulevard  
 Princeton, NJ 08540-5731  
 (609) 452-8060  
 (609) 452-9550 – facsimile  
[rick.sergel@nerc.net](mailto:rick.sergel@nerc.net)  
[david.cook@nerc.net](mailto:david.cook@nerc.net)

/s/ Owen E. MacBride  
 Owen E. MacBride  
 Debra Ann Palmer  
 Schiff Hardin LLP  
 1666 K Street, N.W.  
 Suite 300  
 Washington, DC 20006  
 (202) 778-6400  
 (202) 778-6460 – facsimile  
[omacbride@schiffhardin.com](mailto:omacbride@schiffhardin.com)  
[dpalmer@schiffhardin.com](mailto:dpalmer@schiffhardin.com)

## **Exhibit A**

### **Proposed Violation Risk Factors for Version 1 Reliability Standards**

**Violation Risk Factors — Version 1 Standards Matrix**

The following table lists the Violation Risk Factors (VRFs) for the requirements in the following Version 1 Balancing and Interchange standards:

- BAL-006-1 — Inadvertent Interchange
- INT-001-2 — Interchange Information
- INT-003-1 — Interchange Transaction Information
- INT-004-1 — Interchange Transaction Modification
- INT-005-1 — Interchange Authority Distributes Arranged Interchange
- INT-006-1 — Response to Interchange Authority
- INT-007-1 — Interchange Confirmation
- INT-008-1 — Interchange Authority Distributes Status
- INT-009-1 — Implementation of Interchange
- INT-010-1 — Interchange Coordination Exemptions

These VRFs are the weighted average of the stakeholder VRF selections from the second posting of the Version 1 VRF survey.

<b>BAL-006-1 — Inadvertent Interchange</b>			
BAL-006-1	R1.	Each Balancing Authority shall calculate and record hourly Inadvertent Interchange.	LOWER
BAL-006-1	R2.	Each Balancing Authority shall include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. The Balancing Authority shall take into account interchange served by jointly owned generators.	LOWER
BAL-006-1	R3.	Each Balancing Authority shall ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.	LOWER
BAL-006-1	R4.	Adjacent Balancing Authority Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign. Each Balancing Authority shall compute its Inadvertent Interchange based on the following:	LOWER
BAL-006-1	R4.1.	Each Balancing Authority, by the end of the next business day, shall agree with its Adjacent Balancing Authorities to:	LOWER
BAL-006-1	R4.1.1.	The hourly values of Net Interchange Schedule.	LOWER
BAL-006-1	R4.1.2.	The hourly integrated megawatt-hour values of Net Actual Interchange.	LOWER
BAL-006-1	R4.2.	Each Balancing Authority shall use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.	LOWER
BAL-006-1	R4.3.	A Balancing Authority shall make after-the-fact corrections to the agreed-to daily and monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). Changes or corrections based on non-reliability considerations shall not be reflected in the	LOWER

**Version 1 Violation Risk Factors for Balancing and Interchange Standards BAL-006-1, INT-001-1, INT-003-1 through INT-010-1**

<b>BAL-006-1 — Inadvertent Interchange</b>			
		Balancing Authority's Inadvertent Interchange. After-the-fact corrections to scheduled or actual values will not be accepted without agreement of the Adjacent Balancing Authority(ies).	
BAL-006-1	R5.	Adjacent Balancing Authorities that cannot mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month shall, for the purposes of dispute resolution, submit a report to their respective Regional Reliability Organization Survey Contact. The report shall describe the nature and the cause of the dispute as well as a process for correcting the discrepancy.	LOWER

<b>INT-001-2 — Interchange Information</b>			
INT-001-2	R1.	The Load-Serving, Purchasing-Selling Entity shall ensure that Arranged Interchange is submitted to the Interchange Authority for:	LOWER
INT-001-2	R1.1.	All Dynamic Schedules at the expected average MW profile for each hour.	LOWER
INT-001-2	R2.	The Sink Balancing Authority shall ensure that Arranged Interchange is submitted to the Interchange Authority:	LOWER
INT-001-2	R2.1.	If a Purchasing-Selling Entity is not involved in the Interchange, such as delivery from a jointly owned generator.	LOWER
INT-001-2	R2.2.	For each bilateral Inadvertent Interchange payback.	LOWER

<b>INT-003-1 — Interchange Transaction Information</b>			
INT-003-1	R1.	Each Receiving Balancing Authority shall confirm Interchange Schedules with the Sending Balancing Authority prior to implementation in the Balancing Authority's ACE equation.	MEDIUM
INT-003-1	R1.1.	The Sending Balancing Authority and Receiving Balancing Authority shall agree on Interchange as received from the Interchange Authority, including:	LOWER
INT-003-1	R1.1.1.	Interchange Schedule start and end time.	LOWER
INT-003-1	R1.1.2.	Energy profile.	LOWER
INT-003-1	R1.2.	If a high voltage direct current (HVDC) tie is on the Scheduling Path, then the Sending Balancing Authorities and Receiving Balancing Authorities shall coordinate the Interchange Schedule with the Transmission Operator of the HVDC tie.	MEDIUM

<b>INT-004-1 — Interchange Transaction Modification</b>			
INT-004-1	R1.	At such time as the reliability event allows for the reloading of the transaction, the entity that initiated the curtailment shall release the limit on the Interchange Transaction tag to allow reloading the transaction and shall communicate the release of the limit to the Sink Balancing Authority.	LOWER
INT-004-1	R2.	The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the	LOWER

**Version 1 Violation Risk Factors for Balancing and Interchange Standards BAL-006-1, INT-001-1, INT-003-1 through INT-010-1**

<b>INT-004-1 — Interchange Transaction Modification</b>			
		following occurs:	
INT-004-1	R2.1.	The average energy profile in an hour is greater than 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +10%.	LOWER
INT-004-1	R2.2.	The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +25 megawatt-hours.	LOWER
INT-004-1	R2.3.	A Reliability Coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons.	LOWER

<b>INT-005-1 — Interchange Authority Distributes Arranged Interchange</b>			
INT-005-1	R1.	Prior to the expiration of the time period defined in the Timing Table, Column A, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment to all reliability entities involved in the Interchange.	MEDIUM
INT-005-1	R1.1.	When a Balancing Authority or Reliability Coordinator initiates a Curtailment to Confirmed or Implemented Interchange for reliability, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment only to the Source Balancing Authority and the Sink Balancing Authority.	MEDIUM

<b>INT-006-1 — Response to Interchange Authority</b>			
INT-006-1	R1.	Prior to the expiration of the reliability assessment period defined in the Timing Table, Column B, the Balancing Authority and Transmission Service Provider shall respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	LOWER
INT-006-1	R1.1.	Each involved Balancing Authority shall evaluate the Arranged Interchange with respect to:	LOWER
INT-006-1	R1.1.1.	Energy profile (ability to support the magnitude of the Interchange).	LOWER
INT-006-1	R1.1.2.	Ramp (ability of generation maneuverability to accommodate).	LOWER
INT-006-1	R1.1.3.	Scheduling path (proper connectivity of Adjacent Balancing Authorities).	LOWER
INT-006-1	R1.2.	Each involved Transmission Service Provider shall confirm that the transmission service arrangements associated with the Arranged Interchange have adjacent Transmission Service Provider connectivity, are valid and prevailing transmission system limits will not be violated.	LOWER

<b>INT-007-1 — Interchange Confirmation</b>			
INT-007-1	R1.	The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:	LOWER
INT-007-1	R1.1.	Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).	LOWER
INT-007-1	R1.2.	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.	LOWER
INT-007-1	R1.3.	The following are defined:	LOWER
INT-007-1	R1.3.1.	Generation source and load sink.	LOWER
INT-007-1	R1.3.2.	Megawatt profile.	LOWER
INT-007-1	R1.3.3.	Ramp start and stop times.	LOWER
INT-007-1	R1.3.4.	Interchange duration.	LOWER
INT-007-1	R1.4.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.	LOWER

<b>INT-008-1 — Interchange Authority Distributes Status</b>			
INT-008-1	R1.	Prior to the expiration of the time period defined in the Timing Table, Column C, the Interchange Authority shall distribute to all Balancing Authorities (including Balancing Authorities on both sides of a direct current tie), Transmission Service Providers and Purchasing-Selling Entities involved in the Arranged Interchange whether or not the Arranged Interchange has transitioned to a Confirmed Interchange.	LOWER
INT-008-1	R1.1.	For Confirmed Interchange, the Interchange Authority shall also communicate:	LOWER
INT-008-1	R1.1.1.	Start and stop times, ramps, and megawatt profile to Balancing Authorities.	LOWER
INT-008-1	R1.1.2.	Necessary Interchange information to NERC-identified reliability analysis services.	LOWER

<b>INT-009-1 — Implementation of Interchange</b>			
INT-009-1	R1.	The Balancing Authority shall implement Confirmed Interchange as received from the Interchange Authority.	MEDIUM

<b>INT-010-1 — Interchange Coordination Exemptions</b>			
INT-010-1	R1.	The Balancing Authority that experiences a loss of resources covered by an energy sharing agreement shall ensure that a request for an Arranged Interchange is submitted with a start time no more than 60 minutes beyond the resource loss. If the use of the energy sharing agreement does not exceed 60 minutes from the time of the resource loss, no request for Arranged Interchange	LOWER

**Version 1 Violation Risk Factors for Balancing and Interchange Standards BAL-006-1, INT-001-1, INT-003-1 through INT-010-1**

---

<b>INT-010-1 — Interchange Coordination Exemptions</b>			
		is required.	
INT-010-1	R2.	For a modification to an existing Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit the modified Arranged Interchange reflecting that modification within 60 minutes of the initiation of the event.	LOWER
INT-010-1	R3.	For a new Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit an Arranged Interchange reflecting that Interchange schedule within 60 minutes of the initiation of the event.	LOWER

**Violation Risk Factors — Version 1 Standards Matrix**

The following table lists the Violation Risk Factors (VRFs) for the requirements in the following Version 1 Critical Infrastructure Protection standards:

- CIP-002-1 — Critical Cyber Asset Identification
- CIP-003-1 — Security Management Controls
- CIP-004-1 — Personnel & Training
- CIP-005-1 — Electronic Security Perimeter(s)
- CIP-006-1 — Physical Security of Critical Cyber Assets
- CIP-007-1 — Systems Security Management
- CIP-008-1 — Incident Reporting and Response Planning
- CIP-009-1 — Recovery Plans for Critical Cyber Assets

These VRFs are the weighted average of the stakeholder VRF selections from the second posting of the Version 1 VRF survey.

<b>CIP-002-1 — Critical Cyber Asset Identification</b>			
CIP-002-1	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	LOWER
CIP-002-1	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	LOWER
CIP-002-1	R1.2.	The risk-based assessment shall consider the following assets:	LOWER
CIP-002-1	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	LOWER
CIP-002-1	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.4.	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	LOWER
CIP-002-1	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	LOWER
CIP-002-1	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LOWER
CIP-002-1	R1.2.7.	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	LOWER
CIP-002-1	R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	LOWER
CIP-002-1	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible	MEDIUM

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-002-1 — Critical Cyber Asset Identification</b>			
		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:	
CIP-002-1	R3.1.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	
CIP-002-1	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	LOWER
CIP-002-1	R3.3.	The Cyber Asset is dial-up accessible.	LOWER
CIP-002-1	R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	LOWER

<b>CIP-003-1 — Security Management Controls</b>			
CIP-003-1	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:	LOWER
CIP-003-1	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.	LOWER
CIP-003-1	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	LOWER
CIP-003-1	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-1	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.	LOWER
CIP-003-1	R2.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	LOWER
CIP-003-1	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-1	R2.3.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-1	R3.	Exceptions — Instances where the Responsible Entity cannot	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-003-1 — Security Management Controls</b>			
		conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	
CIP-003-1	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	LOWER
CIP-003-1	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	LOWER
CIP-003-1	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	LOWER
CIP-003-1	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	LOWER
CIP-003-1	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	
CIP-003-1	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	LOWER
CIP-003-1	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	LOWER
CIP-003-1	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-1	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	LOWER
CIP-003-1	R5.1.1.	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	LOWER
CIP-003-1	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	
CIP-003-1	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	LOWER
CIP-003-1	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-1	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-003-1 — Security Management Controls</b>			
		change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	

<b>CIP-004-1 — Personnel &amp; Training</b>			
CIP-004-1	R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: - Direct communications (e.g., emails, memos, computer based training, etc.); - Indirect communications (e.g., posters, intranet, brochures, etc.); - Management support and reinforcement (e.g., presentations, meetings, etc.).	LOWER
CIP-004-1	R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	LOWER
CIP-004-1	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	LOWER
CIP-004-1	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	LOWER
CIP-004-1	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-1	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	
CIP-004-1	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	
CIP-004-1	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	LOWER
CIP-004-1	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	LOWER
CIP-004-1	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	LOWER
CIP-004-1	R3.1.	The Responsible Entity shall ensure that each assessment	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-004-1 — Personnel &amp; Training</b>			
		conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	
CIP-004-1	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	LOWER
CIP-004-1	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.	LOWER
CIP-004-1	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	LOWER
CIP-004-1	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	LOWER
CIP-004-1	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	LOWER

<b>CIP-005-1 — Electronic Security Perimeter(s)</b>			
CIP-005-1	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	MEDIUM
CIP-005-1	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	LOWER
CIP-005-1	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	LOWER
CIP-005-1	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-005-1 — Electronic Security Perimeter(s)</b>			
CIP-005-1	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	LOWER
CIP-005-1	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.	
CIP-005-1	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	LOWER
CIP-005-1	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	LOWER
CIP-005-1	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	MEDIUM
CIP-005-1	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	MEDIUM
CIP-005-1	R2.3.	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-1	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	LOWER
CIP-005-1	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-1	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-1	R2.5.2.	The authentication methods.	LOWER
CIP-005-1	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.	LOWER
CIP-005-1	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-1	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-005-1 — Electronic Security Perimeter(s)</b>			
CIP-005-1	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	LOWER
CIP-005-1	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	LOWER
CIP-005-1	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	LOWER
CIP-005-1	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	LOWER
CIP-005-1	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-1	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	LOWER
CIP-005-1	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	LOWER
CIP-005-1	R4.5.	A review of controls for default accounts, passwords, and network management community strings; and,	LOWER
CIP-005-1	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	LOWER
CIP-005-1	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	LOWER
CIP-005-1	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.	LOWER
CIP-005-1	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	LOWER
CIP-005-1	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.	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-006-1 — Physical Security of Critical Cyber Assets</b>			
CIP-006-1	R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM
CIP-006-1	R1.1.	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.	MEDIUM
CIP-006-1	R1.2.	Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-1	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-1	R1.4.	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-1	R1.5.	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	LOWER
CIP-006-1	R1.6.	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	MEDIUM
CIP-006-1	R1.7.	Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-1	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.	LOWER
CIP-006-1	R1.9.	Process for ensuring that the physical security plan is reviewed at least annually.	LOWER
CIP-006-1	R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	MEDIUM
CIP-006-1	R2.1.	Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.	MEDIUM
CIP-006-1	R2.2.	Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.	MEDIUM

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-006-1 — Physical Security of Critical Cyber Assets</b>			
CIP-006-1	R2.3.	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	MEDIUM
CIP-006-1	R2.4.	Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	MEDIUM
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:	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.	MEDIUM
CIP-006-1	R3.2.	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.	LOWER
CIP-006-1	R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	LOWER
CIP-006-1	R4.1.	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	LOWER
CIP-006-1	R4.2.	Video Recording: Electronic capture of video images of sufficient quality to determine identity.	LOWER
CIP-006-1	R4.3.	Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.	LOWER
CIP-006-1	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.	LOWER
CIP-006-1	R6.	Maintenance and Testing — The Responsible Entity shall implement maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-1	R6.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	LOWER
CIP-006-1	R6.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-006-1 — Physical Security of Critical Cyber Assets</b>			
CIP-006-1	R6.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER

<b>CIP-007-1 — Systems Security Management</b>			
CIP-007-1	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	MEDIUM
CIP-007-1	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	LOWER
CIP-007-1	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-1	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-1	R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	LOWER
CIP-007-1	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MEDIUM
CIP-007-1	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	MEDIUM
CIP-007-1	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER
CIP-007-1	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	LOWER
CIP-007-1	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	LOWER
CIP-007-1	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER
CIP-007-1	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-007-1 — Systems Security Management</b>			
		malware on all Cyber Assets within the Electronic Security Perimeter(s).	
CIP-007-1	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER
CIP-007-1	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.	LOWER
CIP-007-1	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	LOWER
CIP-007-1	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.	
CIP-007-1	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	LOWER
CIP-007-1	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	LOWER
CIP-007-1	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.	LOWER
CIP-007-1	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	LOWER
CIP-007-1	R5.2.1	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	LOWER
CIP-007-1	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-1	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	LOWER
CIP-007-1	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-1	R5.3.1	Each password shall be a minimum of six characters.	LOWER
CIP-007-1	R5.3.2	Each password shall consist of a combination of alpha, numeric,	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-007-1 — Systems Security Management</b>			
		and “special” characters.	
CIP-007-1	R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.	
CIP-007-1	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	LOWER
CIP-007-1	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	LOWER
CIP-007-1	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	LOWER
CIP-007-1	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.	LOWER
CIP-007-1	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-1	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-1	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.	
CIP-007-1	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-1	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-1	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	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:	LOWER
CIP-007-1	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-1	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	LOWER
CIP-007-1	R8.3.	A review of controls for default accounts; and,	LOWER
CIP-007-1	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	LOWER

**Version 1 Violation Risk Factors for Critical Infrastructure Standards CIP-002-1 through CIP-009-1**

<b>CIP-007-1 — Systems Security Management</b>			
CIP-007-1	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	LOWER

<b>CIP-008-1 — Incident Reporting and Response Planning</b>			
CIP-008-1	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	LOWER
CIP-008-1	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER
CIP-008-1	R1.2.	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	LOWER
CIP-008-1	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.	LOWER
CIP-008-1	R1.4.	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	LOWER
CIP-008-1	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-1	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-1	R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	LOWER

<b>CIP-009-1 — Recovery Plans for Critical Cyber Assets</b>			
CIP-009-1	R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	MEDIUM
CIP-009-1	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	MEDIUM
CIP-009-1	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-1	R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	LOWER
CIP-009-1	R3.	Change Control — Recovery plan(s) shall be updated to reflect	LOWER

<b>CIP-009-1 — Recovery Plans for Critical Cyber Assets</b>			
		any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	
CIP-009-1	R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	LOWER
CIP-009-1	R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	LOWER

**Version 1 Violation Risk Factors for Emergency Operations, Transmission Operations, and Voltage Control EOP-005-1, TOP-002-1, VAR-001-1, and VAR-002-1**

**Violation Risk Factors — Version 1 Standards Matrix**

The following table lists the Violation Risk Factors (VRFs) for the requirements in the following Version 1 Emergency Operations, Transmission Operations, and Voltage Control standards:

- EOP-005-1 — System Restoration Plans
- TOP-002-2 — Normal Operations Planning
- VAR-001-1 — Voltage and Reactive Control
- VAR-002-1 — Generator Operations for Maintaining Network Voltage Schedules

These VRFs are the weighted average of the stakeholder VRF selections from the second posting of the Version 1 VRF survey.

<b>EOP-005-1 — System Restoration Plans</b>			
EOP-005-1	R1.	Each Transmission Operator shall have a restoration plan to reestablish its electric system in a stable and orderly manner in the event of a partial or total shutdown of its system, including necessary operating instructions and procedures to cover emergency conditions, and the loss of vital telecommunications channels. Each Transmission Operator shall include the applicable elements listed in Attachment 1-EOP-005 in developing a restoration plan.	MEDIUM
EOP-005-1	R10.	The Transmission Operator shall demonstrate, through simulation or testing, that the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	MEDIUM
EOP-005-1	R10.1.	The Transmission Operator shall perform this simulation or testing at least once every five years.	MEDIUM
EOP-005-1	R11.	Following a disturbance in which one or more areas of the Bulk Electric System become isolated or blacked out, the affected Transmission Operators and Balancing Authorities shall begin immediately to return the Bulk Electric System to normal.	HIGH
EOP-005-1	R11.1.	The affected Transmission Operators and Balancing Authorities shall work in conjunction with their Reliability Coordinator(s) to determine the extent and condition of the isolated area(s).	MEDIUM
EOP-005-1	R11.2.	The affected Transmission Operators and Balancing Authorities shall take the necessary actions to restore Bulk Electric System frequency to normal, including adjusting generation, placing additional generators on line, or load shedding.	HIGH
EOP-005-1	R11.3.	The affected Balancing Authorities, working with their Reliability Coordinator(s), shall immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments as needed to facilitate the restoration. The affected Balancing Authorities shall make all attempts to maintain the adjusted Interchange Schedules, whether generation control is manual or automatic.	HIGH
EOP-005-1	R11.4.	The affected Transmission Operators shall give high priority to restoration of off-site power to nuclear stations.	HIGH
EOP-005-1	R11.5.	The affected Transmission Operators may resynchronize the	MEDIUM

**Version 1 Violation Risk Factors for Emergency Operations, Transmission Operations, and Voltage Control EOP-005-1, TOP-002-1, VAR-001-1, and VAR-002-1**

<b>EOP-005-1 — System Restoration Plans</b>			
		isolated area(s) with the surrounding area(s) when the following conditions are met:	
EOP-005-1	R11.5.1.	Voltage, frequency, and phase angle permit.	HIGH
EOP-005-1	R11.5.2.	The size of the area being reconnected and the capacity of the transmission lines effecting the reconnection and the number of synchronizing points across the system are considered.	HIGH
EOP-005-1	R11.5.3.	Reliability Coordinator(s) and adjacent areas are notified and Reliability Coordinator approval is given.	MEDIUM
EOP-005-1	R11.5.4.	Load is shed in neighboring areas, if required, to permit successful interconnected system restoration.	HIGH
EOP-005-1	R2.	Each Transmission Operator shall review and update its restoration plan at least annually and whenever it makes changes in the power system network, and shall correct deficiencies found during the simulated restoration exercises.	MEDIUM
EOP-005-1	R3.	Each Transmission Operator shall develop restoration plans with a priority of restoring the integrity of the Interconnection.	MEDIUM
EOP-005-1	R4.	Each Transmission Operator shall coordinate its restoration plans with the Generator Owners and Balancing Authorities within its area, its Reliability Coordinator, and neighboring Transmission Operators and Balancing Authorities.	MEDIUM
EOP-005-1	R5.	Each Transmission Operator and Balancing Authority shall periodically test its telecommunication facilities needed to implement the restoration plan.	MEDIUM
EOP-005-1	R6.	Each Transmission Operator and Balancing Authority shall train its operating personnel in the implementation of the restoration plan. Such training shall include simulated exercises, if practicable.	MEDIUM
EOP-005-1	R7.	Each Transmission Operator and Balancing Authority shall verify the restoration procedure by actual testing or by simulation.	MEDIUM
EOP-005-1	R8.	Each Transmission Operator shall verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan requirements for the Transmission Operator's area.	MEDIUM
EOP-005-1	R9.	The Transmission Operator shall document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started and shall provide this documentation for review by the Regional Reliability Organization upon request. Such documentation may include Cranking Path diagrams.	MEDIUM

<b>TOP-002-2 — Normal Operations Planning</b>			
TOP-002-2	R14	Generator Operators shall, without any intentional time delay, notify their Balancing Authority and Transmission Operator of changes in capabilities and characteristics including but not limited to:	MEDIUM
TOP-002-2	R14.1	Changes in real output capabilities.	MEDIUM

**Version 1 Violation Risk Factors for Emergency Operations, Transmission Operations, and Voltage Control EOP-005-1, TOP-002-1, VAR-001-1, and VAR-002-1**

<b>VAR-001-1 — Voltage and Reactive Control</b>			
VAR-001-1	R3	The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.	LOWER
VAR-001-1	R3.1	Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.	LOWER
VAR-001-1	R3.2	For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.	LOWER
VAR-001-1	R4	Each Transmission Operator shall specify a voltage or Reactive Power schedule [1] at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).	MEDIUM
VAR-001-1	R6.1	When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.	MEDIUM
VAR-001-1	R11	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.	LOWER

<b>VAR-002-1 — Generator Operations for Maintaining Network Voltage Schedules</b>			
VAR-002-1	R1	The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator.	MEDIUM
VAR-002-1	R2	Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings[1]) as directed by the Transmission Operator.	MEDIUM
VAR-002-1	R2.1	When a generator's automatic voltage regulator is out of service, the Generator Operator shall use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.	MEDIUM
VAR-002-1	R2.2	When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.	MEDIUM
VAR-002-1	R3	Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:	MEDIUM
VAR-002-1	R3.1	A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator	MEDIUM

**Version 1 Violation Risk Factors for Emergency Operations, Transmission Operations, and Voltage Control EOP-005-1, TOP-002-1, VAR-001-1, and VAR-002-1**

<b>VAR-002-1 — Generator Operations for Maintaining Network Voltage Schedules</b>			
		and power system stabilizer and the expected duration of the change in status or capability.	
VAR-002-1	R3.2	A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.	MEDIUM
VAR-002-1	R4	The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.	LOWER
VAR-002-1	R4.1	For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:	LOWER
VAR-002-1	R4.1.1	Tap settings.	LOWER
VAR-002-1	R4.1.2	Available fixed tap ranges.	LOWER
VAR-002-1	R4.1.3	Impedance data.	LOWER
VAR-002-1	R4.1.4	The +/- voltage range with step-change in % for load-tap changing transformers.	LOWER
VAR-002-1	R5	After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.	MEDIUM
VAR-002-1	R5.1	If the Generator Operator can't comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.	LOWER

**Violation Risk Factors — Version 1 Standards Matrix**

The following table lists the Violation Risk Factors (VRFs) for the requirements in the following Version 1 Facility Ratings standards:

- FAC-008-1 — Facility Ratings Methodology
- FAC-009-1 — Establish and Communicate Facility Ratings
- FAC-010-1 — System Operating Limits Methodology for the Planning Horizon
- FAC-011-1 — System Operating Limits Methodology for the Operations Horizon
- FAC-012-1 — Transfer Capabilities Methodology
- FAC-013-1 — Establish and Communicate Transfer Capabilities
- FAC-014-1 — Establish and Communicate System Operating Limits

These VRFs are the weighted average of the stakeholder VRF selections from the second posting of the Version 1 VRF survey.

<b>FAC-008-1 — Facility Ratings Methodology</b>			
FAC-008-1	R1.	The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:	LOWER
FAC-008-1	R1.1.	A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.	LOWER
FAC-008-1	R1.2.	The method by which the Rating (of major BES equipment that comprises a Facility) is determined.	LOWER
FAC-008-1	R1.2.1.	The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.	LOWER
FAC-008-1	R1.2.2.	The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.	LOWER
FAC-008-1	R1.3.	Consideration of the following:	LOWER
FAC-008-1	R1.3.1.	Ratings provided by equipment manufacturers.	MEDIUM
FAC-008-1	R1.3.2.	Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).	MEDIUM
FAC-008-1	R1.3.3.	Ambient conditions.	MEDIUM
FAC-008-1	R1.3.4.	Operating limitations.	MEDIUM
FAC-008-1	R1.3.5.	Other assumptions.	LOWER
FAC-008-1	R2.	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.	LOWER
FAC-008-1	R3.	If a Reliability Coordinator, Transmission Operator, Transmission	LOWER

<b>FAC-008-1 — Facility Ratings Methodology</b>			
		Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.	

<b>FAC-009-1 — Establish and Communicate Facility Ratings</b>			
FAC-009-1	R1.	The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology.	MEDIUM
FAC-009-1	R2.	The Transmission Owner and Generator Owner shall each provide Facility Ratings for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities to its associated Reliability Coordinator(s), Planning Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities.	MEDIUM

<b>FAC-010-1 — System Operating Limits Methodology for the Planning Horizon</b>			
FAC-010-1	R1	The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:	LOWER
FAC-010-1	R1.1	Be applicable for developing SOLs used in the planning horizon.	LOWER
FAC-010-1	R1.2	State that SOLs shall not exceed associated Facility Ratings.	LOWER
FAC-010-1	R1.3	Include a description of how to identify the subset of SOLs that qualify as IROLs.	LOWER
FAC-010-1	R2	The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:	LOWER
FAC-010-1	R2.1	In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.	MEDIUM
FAC-010-1	R2.2	Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading Outages or uncontrolled separation shall not occur.	MEDIUM
FAC-010-1	R2.2.1	Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.	MEDIUM

**Version 1 Violation Risk Factors for Facility Ratings Standards FAC-008-1 through FAC-014-1**

<b>FAC-010-1 — System Operating Limits Methodology for the Planning Horizon</b>			
FAC-010-1	R2.2.2	Loss of any generator, line, transformer, or shunt device without a Fault.	MEDIUM
FAC-010-1	R2.2.3	Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.	MEDIUM
FAC-010-1	R2.3	Starting with all Facilities in service, the system's response to a single Contingency may include any of the following:	MEDIUM
FAC-010-1	R2.3.1	Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.	MEDIUM
FAC-010-1	R2.3.2	To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.	MEDIUM
FAC-010-1	R2.4	Starting with all facilities in service, the system's response to one of the multiple Contingencies identified in Reliability Standard TPL-003, the system shall demonstrate dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading Outages or uncontrolled separation shall not occur.	MEDIUM
FAC-010-1	R2.5	In determining the system's response to a multiple Contingency, the following shall be acceptable:	MEDIUM
FAC-010-1	R2.5.1	Planned or controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers	MEDIUM
FAC-010-1	R3	The Planning Authority's SOL methodology, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	LOWER
FAC-010-1	R3.1.	Area of study (must include at least the entire Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).	LOWER
FAC-010-1	R3.2.	Selection of applicable Contingencies.	LOWER
FAC-010-1	R3.3.	Level of detail of system models used to determine SOLs.	LOWER
FAC-010-1	R3.4	Allowed uses of Special Protection Systems or Remedial Action Plans.	MEDIUM
FAC-010-1	R3.5	Anticipated transmission system configuration, generation dispatch and Load level.	LOWER
FAC-010-1	R3.6	Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL Tv.	LOWER
FAC-010-1	R4	The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:	LOWER
FAC-010-1	R4.1.	Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.	LOWER
FAC-010-1	R4.2.	Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority	LOWER

**Version 1 Violation Risk Factors for Facility Ratings Standards FAC-008-1 through FAC-014-1**

<b>FAC-010-1 — System Operating Limits Methodology for the Planning Horizon</b>			
		Area.	
FAC-010-1	R4.3.	Each Transmission Planner that works in the Planning Authority's Planning Authority Area.	LOWER
FAC-010-1	R5	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	LOWER

<b>FAC-011-1 — System Operating Limits Methodology for the Operations Horizon</b>			
FAC-011-1	R1	The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:	LOWER
FAC-011-1	R1.1	Be applicable for developing SOLs used in the operations horizon.	LOWER
FAC-011-1	R1.2	State that SOLs shall not exceed associated Facility Ratings.	LOWER
FAC-011-1	R1.3	Include a description of how to identify the subset of SOLs that qualify as IROLs.	LOWER
FAC-011-1	R2	The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:	MEDIUM
FAC-011-1	R2.1	In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.	MEDIUM
FAC-011-1	R2.2	Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading Outages or uncontrolled separation shall not occur.	MEDIUM
FAC-011-1	R2.2.1	Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.	MEDIUM
FAC-011-1	R2.2.2	Loss of any generator, line, transformer, or shunt device without a Fault.	MEDIUM
FAC-011-1	R2.2.3	Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.	MEDIUM
FAC-011-1	R2.3	In determining the system's response to a single Contingency, the following shall be acceptable:	MEDIUM
FAC-011-1	R2.3.1	Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.	MEDIUM
FAC-011-1	R2.3.2	Interruption of other network customers, only if the system has already been adjusted, or is being adjusted, following at least one	MEDIUM

**Version 1 Violation Risk Factors for Facility Ratings Standards FAC-008-1 through FAC-014-1**

<b>FAC-011-1 — System Operating Limits Methodology for the Operations Horizon</b>			
		prior outage, or, if the real-time operating conditions are more adverse than anticipated in the corresponding studies, e.g., load greater than studied.	
FAC-011-1	R2.3.3	System reconfiguration through manual or automatic control or protection actions.	MEDIUM
FAC-011-1	R2.4	To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.	MEDIUM
FAC-011-1	R3	The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	MEDIUM
FAC-011-1	R3.1.	Area of study (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)	MEDIUM
FAC-011-1	R3.2.	Selection of applicable Contingencies.	MEDIUM
FAC-011-1	R3.3.	A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for real-time use given the real-time system conditions. The process shall address recalculating these stability limits and expanding this list of stability limits and the list of stability-related multiple contingencies.	MEDIUM
FAC-011-1	R3.4	Level of detail of system models used to determine SOLs.	
FAC-011-1	R3.5	Allowed uses of Special Protection Systems or Remedial Action Plans.	MEDIUM
FAC-011-1	R3.6	Anticipated transmission system configuration, generation dispatch and Load level.	MEDIUM
FAC-011-1	R3.7	Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL Tv.	MEDIUM
FAC-011-1	R4	The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:	LOWER
FAC-011-1	R4.1.	Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.	LOWER
FAC-011-1	R4.2.	Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.	LOWER
FAC-011-1	R4.3.	Each Transmission Operator that operates in the Reliability Coordinator Area.	LOWER
FAC-011-1	R5	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL	LOWER

**Version 1 Violation Risk Factors for Facility Ratings Standards FAC-008-1 through FAC-014-1**

<b>FAC-011-1 — System Operating Limits Methodology for the Operations Horizon</b>			
		Methodology and, if no change will be made to that SOL Methodology, the reason why.	

<b>FAC-012-1 — Transfer Capabilities Methodology</b>			
FAC-012-1	R1.	The Reliability Coordinator and Planning Authority shall each document its current methodology used for developing its inter-regional and intra-regional Transfer Capabilities (Transfer Capability Methodology). The Transfer Capability Methodology shall include all of the following:	LOWER
FAC-012-1	R1.1.	A statement that Transfer Capabilities shall respect all applicable System Operating Limits (SOLs).	LOWER
FAC-012-1	R1.2.	A definition stating whether the methodology is applicable to the planning horizon or the operating horizon.	
FAC-012-1	R1.3.	A description of how each of the following is addressed, including any reliability margins applied to reflect uncertainty with projected BES conditions:	LOWER
FAC-012-1	R1.3.1.	Transmission system topology	LOWER
FAC-012-1	R1.3.2.	System demand	LOWER
FAC-012-1	R1.3.3.	Generation dispatch	LOWER
FAC-012-1	R1.3.4.	Current and projected transmission uses	LOWER
FAC-012-1	R2.	The Reliability Coordinator shall issue its Transfer Capability Methodology, and any changes to that methodology, prior to the effectiveness of such changes, to all of the following:	LOWER
FAC-012-1	R2.1	Each Adjacent Reliability Coordinator and each Reliability Coordinator that indicated a reliability-related need for the methodology.	LOWER
FAC-012-1	R2.2	Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.	
FAC-012-1	R2.3	Each Transmission Operator that operates in the Reliability Coordinator Area.	LOWER
FAC-012-1	R3.	The Planning Authority shall issue its Transfer Capability Methodology, and any changes to that methodology, prior to the effectiveness of such changes, to all of the following:	LOWER
FAC-012-1	R3.1.	Each Transmission Planner that works in the Planning Authority's Planning Authority Area.	LOWER
FAC-012-1	R3.2.	Each Adjacent Planning Authority and each Planning Authority that indicated a reliability-related need for the methodology.	LOWER
FAC-012-1	R3.3.	Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.	LOWER
FAC-012-1	R4.	If a recipient of the Transfer Capability Methodology provides documented technical comments on the methodology, the Reliability Coordinator or Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability Methodology and,	LOWER

**Version 1 Violation Risk Factors for Facility Ratings Standards FAC-008-1 through FAC-014-1**

<b>FAC-012-1 — Transfer Capabilities Methodology</b>			
		if no change will be made to that Transfer Capability Methodology, the reason why.	

<b>FAC-013-1 — Establish and Communicate Transfer Capabilities</b>			
FAC-013-1	R1.	The Reliability Coordinator and Planning Authority shall each establish a set of inter-regional and intra-regional Transfer Capabilities that is consistent with its current Transfer Capability Methodology.	MEDIUM
FAC-013-1	R2.	The Reliability Coordinator and Planning Authority shall each provide its inter-regional and intra-regional Transfer Capabilities to those entities that have a reliability-related need for such Transfer Capabilities and make a written request that includes a schedule for delivery of such Transfer Capabilities as follows:	MEDIUM
FAC-013-1	R2.1.	The Reliability Coordinator shall provide its Transfer Capabilities to its associated Regional Reliability Organization(s), to its adjacent Reliability Coordinators, and to the Transmission Operators, Transmission Service Providers and Planning Authorities that work in its Reliability Coordinator Area.	MEDIUM
FAC-013-1	R2.2.	The Planning Authority shall provide its Transfer Capabilities to its associated Reliability Coordinator(s) and Regional Reliability Organization(s), and to the Transmission Planners and Transmission Service Provider(s) that work in its Planning Authority Area.	MEDIUM

<b>FAC-014-1 — Establish and Communicate System Operating Limits</b>			
FAC-014-1	R1	The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.	MEDIUM
FAC-014-1	R2	The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology.	MEDIUM
FAC-014-1	R3	The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology.	MEDIUM
FAC-014-1	R4	The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology.	MEDIUM
FAC-014-1	R5	The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows:	MEDIUM
FAC-014-1	R5.1	The Reliability Coordinator shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Reliability	MEDIUM

<b>FAC-014-1 — Establish and Communicate System Operating Limits</b>			
		Coordinators and Reliability Coordinators who indicate a reliability-related need for those limits, and to the Transmission Operators, Transmission Planners, Transmission Service Providers and Planning Authorities within its Reliability Coordinator Area. For each IROL, the Reliability Coordinator shall provide the following supporting information:	
FAC-014-1	R5.1.1	Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL.	MEDIUM
FAC-014-1	R5.1.2	The value of the IROL and its associated Tv.	MEDIUM
FAC-014-1	R5.1.3	The associated Contingency(ies).	MEDIUM
FAC-014-1	R5.1.4	The type of limitation represented by the IROL (e.g., voltage collapse, angular stability).	MEDIUM
FAC-014-1	R5.2	The Transmission Operator shall provide any SOLs it developed to its Reliability Coordinator and to the Transmission Service Providers that share its portion of the Reliability Coordinator Area.	MEDIUM
FAC-014-1	R5.3	The Planning Authority shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Planning Authorities, and to Transmission Planners, Transmission Service Providers, Transmission Operators and Reliability Coordinators that work within its Planning Authority Area.	MEDIUM
FAC-014-1	R5.4	The Transmission Planner shall provide its SOLs (including the subset of SOLs that are IROLs) to its Planning Authority, Reliability Coordinators, Transmission Operators, and Transmission Service Providers that work within its Transmission Planning Area and to adjacent Transmission Planners.	MEDIUM
FAC-014-1	R6	The Planning Authority shall identify the subset of multiple contingencies from Reliability Standard TPL-003 which result in stability limits.	MEDIUM
FAC-014-1	R6.1	The Planning Authority shall provide this list of multiple contingencies and the associated stability limits to the Reliability Coordinators that monitor the facilities associated with these contingencies and limits.	MEDIUM

**Violation Risk Factors — Version 1 Standards Matrix**

The following table lists the Violation Risk Factors (VRFs) for the requirements in the following Version 1 Interconnection Reliability Operations standards:

- IRO-014-1 — Procedures to Support Coordination Between Reliability Coordinators
- IRO-015-1 — Notifications and Information Exchange Between Reliability Coordinators
- IRO-016-1 — Coordination of Real-time Activities Between Reliability Coordinators

These VRFs are the weighted average of the stakeholder VRF selections from the second posting of the Version 1 VRF survey.

<b>IRO-014-1 — Procedures to Support Coordination Between Reliability Coordinators</b>			
IRO-014-1	R1.	The Reliability Coordinator shall have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability. These Operating Procedures, Processes, or Plans shall address Scenarios that affect other Reliability Coordinator Areas as well as those developed in coordination with other Reliability Coordinators.	MEDIUM
IRO-014-1	R1.1.	These Operating Procedures, Processes, or Plans shall collectively address, as a minimum, the following:	LOWER
IRO-014-1	R1.1.1.	Communications and notifications, including the conditions under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators. Examples of conditions when one Reliability Coordinator may need to notify another Reliability Coordinator may include (but aren't limited to) sabotage events, Interconnection Reliability Operating Limit violations, voltage reductions, insufficient resources, arming of special protection systems, etc.	MEDIUM
IRO-014-1	R1.1.2.	Energy and capacity shortages.	MEDIUM
IRO-014-1	R1.1.3.	Planned or unplanned outage information.	MEDIUM
IRO-014-1	R1.1.4.	Voltage control, including the coordination of reactive resources for voltage control.	MEDIUM
IRO-014-1	R2.	Each Reliability Coordinator's Operating Procedure, Process, or Plan that requires one or more other Reliability Coordinators to take action (e.g., make notifications, exchange information, or coordinate actions) shall be:	LOWER
IRO-014-1	R2.1.	Agreed to by all the Reliability Coordinators required to take the indicated action(s).	LOWER
IRO-014-1	R2.2.	Distributed to all Reliability Coordinators that are required to take the indicated action(s).	LOWER
IRO-014-1	R3.	A Reliability Coordinator's Operating Procedures, Processes, or Plans developed to support a Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan shall include:	

**Version 1 Violation Risk Factors for Interconnection Reliability Operations Standards IRO-014-1 through IRO-016-1**

<b>IRO-014-1 — Procedures to Support Coordination Between Reliability Coordinators</b>			
IRO-014-1	R3.1.	A reference to the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	MEDIUM
IRO-014-1	R3.2.	The agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	LOWER
IRO-014-1	R4.	Each of the Operating Procedures, Processes, and Plans addressed in Reliability Standard IRO-014 Requirement 1 and Requirement 3 shall:	LOWER
IRO-014-1	R4.1.	Include version control number or date	LOWER
IRO-014-1	R4.2.	Include a distribution list.	LOWER
IRO-014-1	R4.3.	Be reviewed, at least once every three years, and updated if needed.	LOWER
IRO-014-7	R1.1.5.	Coordination of information exchange to support reliability assessments.	LOWER
IRO-014-8	R1.1.6.	Authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas.	LOWER

<b>IRO-015-1 — Notifications and Information Exchange Between Reliability Coordinators</b>			
IRO-015-1	R1.	The Reliability Coordinator shall follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators.	MEDIUM
IRO-015-1	R1.1.	The Reliability Coordinator shall make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas.	MEDIUM
IRO-015-1	R2.	The Reliability Coordinator shall participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.	LOWER
IRO-015-1	R2.1.	The frequency of these conference calls shall be agreed upon by all involved Reliability Coordinators and shall be at least weekly.	LOWER
IRO-015-1	R3.	The Reliability Coordinator shall provide reliability-related information as requested by other Reliability Coordinators.	MEDIUM

<b>IRO-016-1 — Coordination of Real-time Activities Between Reliability Coordinators</b>			
IRO-016-1	R1.	The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.	MEDIUM
IRO-016-1	R1.1.	If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.	MEDIUM
IRO-016-1	R1.2.	If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the	MEDIUM

**Version 1 Violation Risk Factors for Interconnection Reliability Operations Standards IRO-014-1 through IRO-016-1**

---

<b>IRO-016-1 — Coordination of Real-time Activities Between Reliability Coordinators</b>			
		causes of the disagreement (bad data, status, study results, tools, etc.).	
IRO-016-1	R1.2.1.	If time permits, this re-evaluation shall be done before taking corrective actions.	MEDIUM
IRO-016-1	R1.2.2.	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.	MEDIUM
IRO-016-1	R1.3.	If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.	MEDIUM
IRO-016-1	R2.	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.	LOWER

**Violation Risk Factors — Version 1 Standards Matrix**

The following table lists the Violation Risk Factors (VRFs) for the requirements in the following Version 1 Modeling standards:

MOD-013 — Maintenance and Distribution of Dynamics Data Requirements and Reporting Procedures

MOD-016 — Documentation of Data Reporting Requirements for Actual and Forecast Demands, Net Energy for Load, and Controllable Demand-side Management

MOD-024 — Verification of Generator Gross and Net Real Power Capability

MOD-025 — Verification of Generator Gross and Net Reactive Power Capability

These VRFs are the weighted average of the stakeholder VRF selections from the second posting of the Version 1 VRF survey.

<b>MOD-013 — Maintenance and Distribution of Dynamics Data Requirements and Reporting Procedures</b>			
MOD-013-1	R1.	The Regional Reliability Organization, in coordination with its Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners, shall develop comprehensive dynamics data requirements and reporting procedures needed to model and analyze the dynamic behavior or response of each of the NERC Interconnections: Eastern, Western, and ERCOT. Within an Interconnection, the Regional Reliability Organizations shall jointly coordinate on the development of the data requirements and reporting procedures for that Interconnection. Each set of Interconnection-wide dynamics data requirements shall include the following dynamics data requirements:	MEDIUM
MOD-013-1	R1.1.	Design data shall be provided for new or refurbished excitation systems (for synchronous generators and synchronous condensers) at least three months prior to the installation date.	MEDIUM
MOD-013-1	R1.1.1.	If design data is unavailable from the manufacturer 3 months prior to the installation date, estimated or typical manufacturer's data, based on excitation systems of similar design and characteristics, shall be provided.	LOWER
MOD-013-1	R1.2.	Unit-specific dynamics data shall be reported for generators and synchronous condensers (including, as appropriate to the model, items such as inertia constant, damping coefficient, saturation parameters, and direct and quadrature axes reactances and time constants), excitation systems, voltage regulators, turbine-governor systems, power system stabilizers, and other associated generation equipment.	MEDIUM
MOD-013-1	R1.2.1.	Estimated or typical manufacturer's dynamics data, based on units of similar design and characteristics, may be submitted when unit-specific dynamics data cannot be obtained. In no case shall other than unit-specific data be reported for generator units installed after 1990.	MEDIUM
MOD-013-1	R1.2.2.	The Interconnection-wide requirements shall specify unit size thresholds for permitting: The use of non-detailed vs. detailed models, The netting of small generating units with bus load, and	LOWER

<b>MOD-013 — Maintenance and Distribution of Dynamics Data Requirements and Reporting Procedures</b>			
		The combining of multiple generating units at one plant.	
MOD-013-1	R1.3.	Device specific dynamics data shall be reported for dynamic devices, including, among others, static VAR controllers, high voltage direct current systems, flexible AC transmission systems, and static compensators.	MEDIUM
MOD-013-1	R1.4.	Dynamics data representing electrical Demand characteristics as a function of frequency and voltage.	LOWER
MOD-013-1	R1.5.	Dynamics data shall be consistent with the reported steady-state (power flow) data supplied per Reliability Standard MOD-010 Requirement 1.	MEDIUM
MOD-013-1	R2.	The Regional Reliability Organization shall participate in the documentation of its Interconnection's data requirements and reporting procedures and, shall participate in the review of those data requirements and reporting procedures (at least every five years), and shall provide those data requirements and reporting procedures to Regional Reliability Organizations, NERC, and all users of the Interconnected systems on request (within five business days).	LOWER

<b>MOD-016 — Documentation of Data Reporting Requirements for Actual and Forecast Demands, Net Energy for Load, and Controllable Demand-side Management</b>			
MOD-016-1	R1.	The Planning Authority and Regional Reliability Organization shall have documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses.	LOWER
MOD-016-1	R1.1.	The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021. The data submittal requirements shall stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.	LOWER
MOD-016-1	R2.	The Regional Reliability Organization shall distribute its documentation required in Requirement 1 and any changes to that documentation, to all Planning Authorities that work within its Region. the Regional Reliability Organization shall make this distribution within 30 calendar days of approval. The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area. The Planning Authority shall make this distribution within 30 calendar days of approval.	LOWER

<b>MOD-024 — Verification of Generator Gross and Net Real Power Capability</b>			
MOD-024-1	R1.	The Regional Reliability Organization shall establish and maintain procedures to address verification of generator gross and net Real Power capability. These procedures shall include the following:	MEDIUM
MOD-024-1	R1.1.	Generating unit exemption criteria including documentation of those units that are exempt from a portion or all of these procedures.	MEDIUM
MOD-024-1	R1.2.	Criteria for reporting generating unit auxiliary loads.	LOWER
MOD-024-1	R1.3.	Acceptable methods for model and data verification, including any applicable conditions under which the data should be verified. Such methods can include use of manufacturer data, commissioning data, performance tracking, and testing, etc.	MEDIUM
MOD-024-1	R1.4.	Periodicity and schedule of model and data verification and reporting.	MEDIUM
MOD-024-1	R1.5.	Information to be verified and reported:	MEDIUM
MOD-024-1	R1.5.1.	Seasonal gross and net Real Power generating capabilities.	MEDIUM
MOD-024-1	R1.5.2.	Real power requirements of auxiliary loads.	LOWER
MOD-024-1	R1.5.3.	Method of verification, including date and conditions.	MEDIUM
MOD-024-1	R2.	The Regional Reliability Organization shall provide its generator gross and net Real Power capability verification and reporting procedures, and any changes to those procedures, to the Generator Owners, Generator Operators, Transmission Operators, Planning Authorities, and Transmission Planners affected by the procedure within 30 calendar days of the approval.	LOWER
MOD-024-1	R3.	The Generator Owner shall follow its Regional Reliability Organization's procedures for verifying and reporting its gross and net Real Power generating capability per R1.	MEDIUM

<b>MOD-025 — Verification of Generator Gross and Net Reactive Power Capability</b>			
MOD-025-1	R1.	The Regional Reliability Organization shall establish and maintain procedures to address verification of generator gross and net Reactive Power capability. These procedures shall include the following:	LOWER
MOD-025-1	R1.1.	Generating unit exemption criteria including documentation of those units that are exempt from a portion or all of these procedures.	LOWER
MOD-025-1	R1.2.	Criteria for reporting generating unit auxiliary loads.	LOWER
MOD-025-1	R1.3.	Acceptable methods for model and data verification, including any applicable conditions under which the data should be verified. Such methods can include use of commissioning data, performance tracking, engineering analysis, testing, etc.	LOWER
MOD-025-1	R1.4.	Periodicity and schedule of model and data verification and reporting.	LOWER
MOD-025-1	R1.5.	Information to be reported:	LOWER
MOD-025-1	R1.5.1.	Verified maximum gross and net Reactive Power capability (both lagging and leading) at Seasonal Real Power generating	LOWER

**Version 1 Violation Risk Factors for Modeling Standards MOD-013-1, MOD-016-1, MOD-024-1, MOD-025-1**

---

<b>MOD-025 — Verification of Generator Gross and Net Reactive Power Capability</b>			
		capabilities as reported in accordance with Reliability Standard MOD-024 Requirement 1.5.1.	
MOD-025-1	R1.5.2.	Verified Reactive Power limitations, such as generator terminal voltage limitations, shorted rotor turns, etc.	LOWER
MOD-025-1	R1.5.2.	Verified Reactive Power of auxiliary loads.	LOWER
MOD-025-1	R1.5.4.	Method of verification, including date and conditions.	LOWER
MOD-025-1	R2.	The Regional Reliability Organization shall provide its generator gross and net Reactive Power capability verification and reporting procedures, and any changes to those procedures, to the Generator Owners, Generator Operators, Transmission Operators, Planning Authorities, and Transmission Planners affected by the procedure within 30 calendar days of the approval.	LOWER
MOD-025-1	R3.	The Generator Owner shall follow its Regional Reliability Organization's procedures for verifying and reporting its gross and net Reactive Power generating capability per R1.	LOWER

**Violation Risk Factors — Version 1 Standards Matrix**

The following table lists the Violation Risk Factors (VRFs) for the requirements in the following Version 1 Protection and Control standards:

- PRC-002-1 — Define and Document Disturbance Monitoring Equipment Requirements
- PRC-018-1 — Disturbance Monitoring Equipment Installation and Data Reporting
- PRC-021-1 — Under-Voltage Load Shedding Program Data
- PRC-022-1 — Under-Voltage Load Shedding Program Performance

These VRFs are the weighted average of the stakeholder VRF selections from the second posting of the Version 1 VRF survey.

<b>PRC-002-1 — Define and Document Disturbance Monitoring Equipment Requirements</b>			
PRC-002-1	R1	The Regional Reliability Organization shall establish the following installation requirements for sequence of event recording:	LOWER
PRC-002-1	R1.1	Location, monitoring and recording requirements, including the following:	LOWER
PRC-002-1	R1.1.1.	Criteria for equipment location (e.g., by voltage, geographic area, station size, etc.).	LOWER
PRC-002-1	R1.1.2.	Devices to be monitored.	LOWER
PRC-002-1	R2	The Regional Reliability Organization shall establish the following installation requirements for fault recording:	LOWER
PRC-002-1	R2.1	Location, monitoring and recording requirements, including the following:	LOWER
PRC-002-1	R2.1.1	Criteria for equipment location (e.g., by voltage, geographic area, station size, etc.).	LOWER
PRC-002-1	R2.1.2	Elements to be monitored at each location.	LOWER
PRC-002-1	R2.1.3	Electrical quantities to be recorded for each monitored element shall be sufficient to determine the following:	LOWER
PRC-002-1	R2.1.3.1	Three phase to neutral voltages.	LOWER
PRC-002-1	R2.1.3.2	Three phase currents and neutral currents.	LOWER
PRC-002-1	R2.1.3.3	Polarizing currents and voltages, if used.	LOWER
PRC-002-1	R2.1.3.4	Frequency.	LOWER
PRC-002-1	R2.1.3.5	Megawatts and megavars.	LOWER
PRC-002-1	R2.2	Technical requirements, including the following:	LOWER
PRC-002-1	R2.2.1	Recording duration requirements.	LOWER
PRC-002-1	R2.2.2	Minimum sampling rate of 16 samples per cycle.	LOWER
PRC-002-1	R2.2.3	Event triggering requirements.	LOWER
PRC-002-1	R3	The Regional Reliability Organization shall establish the following installation requirements for dynamic Disturbance recording:	LOWER
PRC-002-1	R3.1.	Location, monitoring and recording requirements including the following:	LOWER
PRC-002-1	R3.1.1	Criteria for equipment location giving consideration to the following:	LOWER

PRC-002-1 — Define and Document Disturbance Monitoring Equipment Requirements			
		<ul style="list-style-type: none"> <li>- Site(s) in or near major load centers</li> <li>- Site(s) in or near major generation clusters</li> <li>- Site(s) in or near major voltage sensitive areas</li> <li>- Site(s) on both sides of major transmission interfaces</li> <li>- A major transmission junction</li> <li>- Elements associated with Interconnection Reliability Operating Limits</li> <li>- Major EHV interconnections between control areas</li> <li>- Coordination with neighboring regions within the interconnection</li> </ul>	
PRC-002-1	R3.1.2	Elements and number of phases to be monitored at each location.	LOWER
PRC-002-1	R3.1.3	Electrical quantities to be recorded for each monitored element shall be sufficient to determine the following:	LOWER
PRC-002-1	R3.1.3.1	Voltage, current and frequency.	LOWER
PRC-002-1	R3.1.3.2	Megawatts and megavars.	LOWER
PRC-002-1	R3.2.	Technical requirements, including the following:	LOWER
PRC-002-1	R3.2.1	Capability for continuous recording for devices installed after January 1, 2009.	LOWER
PRC-002-1	R3.2.2	Each device shall sample data at a rate of at least 960 samples per second and shall record the RMS value of electrical quantities at a rate of at least 6 records per second.	LOWER
PRC-002-1	R4	The Regional Reliability Organization shall establish requirements for facility owners to report Disturbance data recorded by their DME installations. The Disturbance data reporting requirements shall include the following:	LOWER
PRC-002-1	R4.1.	Criteria for events that require the collection of data from DMEs.	LOWER
PRC-002-1	R4.2.	List of entities that must be provided with recorded Disturbance data.	LOWER
PRC-002-1	R4.3.	Timetable for response to data request.	LOWER
PRC-002-1	R4.4	Provision for reporting Disturbance data in a format which is capable of being viewed, read and analyzed with a generic COMTRADE[1] analysis tool,	LOWER
PRC-002-1	R4.5	Naming of data files in conformance with the IEEE C37.232 Recommended Practice for Naming Time Sequence Data Files[2].	LOWER
PRC-002-1	R4.6	Data content requirements and guidelines.	LOWER
PRC-002-1	R5	The Regional Reliability Organization shall provide its requirements (and any revisions to those requirements) including those for DME installation and Disturbance data reporting to the affected Transmission Owners and Generator Owners within 30 calendar days of approval of those requirements.	LOWER
PRC-002-1	R6	The Regional Reliability Organization shall periodically (at least every five years) review, update and approve its Regional requirements for Disturbance monitoring and reporting.	LOWER

PRC-018-1 — Disturbance Monitoring Equipment Installation and Data Reporting			
PRC-018-1	R1	Each Transmission Owner and Generator Owner required to install DMEs by its Regional Reliability Organization (reliability standard PRC-002 Requirements 1-3) shall have DMEs installed that meet the following requirements:	LOWER
PRC-018-1	R1.1	Internal Clocks in DME devices shall be synchronized to within 2 milliseconds or less of Universal Coordinated Time scale (UTC)	LOWER
PRC-018-1	R1.2	Recorded data from each Disturbance shall be retrievable for ten calendar days..	LOWER
PRC-018-1	R2	The Transmission Owner and Generator Owner shall each install DMEs in accordance with its Regional Reliability Organization's installation requirements (reliability standard PRC-002 Requirements 1 through 3).	LOWER
PRC-018-1	R3	The Transmission Owner and Generator Owner shall each maintain, and report to its Regional Reliability Organization on request, the following data on the DMEs installed to meet that region's installation requirements (reliability standard PRC-002 Requirements 1.1, 2.1 and 3.1):	LOWER
PRC-018-1	R3.1	Type of DME (sequence of event recorder, fault recorder, or dynamic disturbance recorder).	LOWER
PRC-018-1	R3.2	Make and model of equipment.	LOWER
PRC-018-1	R3.3	Installation location.	LOWER
PRC-018-1	R3.4	Operational status.	LOWER
PRC-018-1	R3.5	Date last tested.	LOWER
PRC-018-1	R3.6	Monitored elements, such as transmission circuit, bus section, etc.	LOWER
PRC-018-1	R3.7	Monitored devices, such as circuit breaker, disconnect status, alarms, etc.	LOWER
PRC-018-1	R3.8	Monitored electrical quantities, such as voltage, current, etc.	LOWER
PRC-018-1	R4	The Transmission Owner and Generator Owner shall each provide Disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements (reliability standard PRC-002 Requirement 4).	LOWER
PRC-018-1	R5	The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years.	LOWER
PRC-018-1	R6	Each Transmission Owner and Generator Owner that is required by its Regional Reliability Organization to have DMEs shall have a maintenance and testing program for those DMEs that includes:	LOWER
PRC-018-1	R6.1	Maintenance and testing intervals and their basis.	LOWER
PRC-018-1	R6.2	Summary of maintenance and testing procedures.	LOWER

<b>PRC-021-1 — Under-Voltage Load Shedding Program Data</b>			
PRC-021-1	R1.	Each Transmission Owner and Distribution Provider that owns a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall annually update its UVLS data to support the Regional UVLS program database. The following data shall be provided to the Regional Reliability Organization for each installed UVLS system:	LOWER
PRC-021-1	R1.1.	Size and location of customer load, or percent of connected load, to be interrupted.	LOWER
PRC-021-1	R1.2.	Corresponding voltage set points and overall scheme clearing times.	LOWER
PRC-021-1	R1.3.	Time delay from initiation to trip signal.	LOWER
PRC-021-1	R1.4.	Breaker operating times.	LOWER
PRC-021-1	R1.5.	Any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	LOWER
PRC-021-1	R2.	Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request.	LOWER

<b>PRC-022-1 — Under-Voltage Load Shedding Program Performance</b>			
PRC-022-1	R1.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:	LOWER
PRC-022-1	R1.1.	A description of the event including initiating conditions.	LOWER
PRC-022-1	R1.2.	A review of the UVLS set points and tripping times.	LOWER
PRC-022-1	R1.3.	A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.	LOWER
PRC-022-1	R1.4.	A summary of the findings.	LOWER
PRC-022-1	R1.5.	For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.	MEDIUM
PRC-022-1	R2.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.	LOWER

**Exhibit B**  
**Record of Development**  
**(Provided Separately)**

**Exhibit C**  
**Standards Drafting Team Roster**

## Violation Risk Factors Drafting Team

<b>Chairman</b>	Stanley E. Kopman Director, Planning & Compliance	Northeast Power Coordinating Council 1515 Broadway 43rd Floor New York, New York 10036-8901	(212) 840-1070 (212) 302-2782 Fx skopman@npcc.org
<b>NERC Staff</b>	Timothy Kucey Manager of Enforcement & Mitigation	North American Electric Reliability Council 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx tim.kucey@ nerc.net
	Terry Bilke Technical Manager	Midwest ISO, Inc. 701 City Center Drive Carmel, Indiana 46032	(317) 249-5463 (317) 249-5910 Fx tbilke@ midwestiso.org
	Shannon Black	Sacramento Municipal Utility District 6301 S Street Sacramento, California 95817	(916) 732-5734 sblack@smud.org
	Cary B. Deise Director, Transmission Operations and Planning	Arizona Public Service Co. M.S. 2260 P.O. Box 53999 Phoenix, Arizona 85072-3999	(602) 250-1232 (602) 250-1155 Fx cary.deise@ aps.com
	Rod C. Hardiman Project Manager, Reliability & Risk Analysis Group Transmission Planning	Southern Company Services, Inc. 600 N. 18th Street P.O. Box 2641 Birmingham, Alabama 35291	(205) 257-7056 (205) 257-1040 Fx rhardim@ southernco.com
	Douglas F. Johnson Compliance Officer	American Transmission Company, LLC N19 W23993 Ridgeview Parkway West P.O. Box 47 Waukesha, Wisconsin 53188	(262) 506-6863 dfjohnson@ atllc.com
	Richard J. Kafka Transmission Policy Manager	Potomac Electric Power Co. P.O. Box 341010 Bethesda, Maryland 3410120827-1010	(301) 469-5274 (301) 469-5235 Fx rjkafka@ pepcoholdings.com
	Joseph J. Krupar Operations Consultant	Florida Municipal Power Agency 8553 Commodity Circle Orlando, Florida 32819-9002	(407) 355-5793 (407) 355-5793 Fx joe.krupar@ fmpa.com
	Greg Lange Chief Dispatcher	Grant County PUD No. 2 P.O. Box 878 Ephrata, Washington 98823	(509) 754-5061 (509) 754-5392 Fx glange@gcpud.org
	Norbert D. Mizwicki Senior Consultant - Operations	ReliabilityFirst Corporation 939 Parkview Boulevard Lombard, Illinois 60148-3267	(630) 261-2657 (630) 691-4222 Fx norb.mizwicki@ rfirst.org

	Jim R. Nickel Senior Engineer	Michigan Public Power Agency 809 Centennial Way Lansing, Michigan 48917	(517) 323-8919 (517) 323-8373 Fx jnickel@ mpower.org
	Eric Senkowicz	Florida Reliability Coordinating Council 1408 N. Westshore Blvd Suite 1002 Tampa, Florida 33607	(813) 289-5644 esenkowicz@ frcc.com
	Philip Scott Sobol Senior Corporate Security Consultant	Corporate Risk Solutions, Inc. 8725 Rosehill Rd Lenexa, Kansas 66215	(913) 322-5402 psobol@ corprisk.net
<b>SAC Liason</b>	James Spearman Executive Assistant & Senior Technical Advisor	Public Service Commission of South Carolina 101 Executive Center Drive Suite 100 P.O. Drawer 11649 Columbia, South Carolina 29211	(803) 896-5142 (803) 896-5231 Fx james.spearman@ psc.sc.gov
	James R. Stanton Director of Reliability Compliance	Calpine Corporation 4100 Underwood Road Pasadena, Texas 77507	(832) 476-4453 (281) 291-7089 Fx jstanton@ calpine.com
	Gerald Steffens Manager of Operations/Reliability	Rochester Public Utilities	(507) 280-1607 (507) 280-1542 Fx gsteffens@ rpu.org
	John C. Stephens	FirstEnergy Corp. 76 South Main Street Akron, Ohio 44308	(330) 384-5356 stephensj@ firstenergycorp.com
	Charles V. Waits Vice President-Operations and Transmission Strategy	Michigan Electric Transmission Company 540 Avis Drive, Suite H Ann Arbor, Michigan 48108	(734) 929-1227 (734) 929-1212 Fx cwaits@ metcllc.com
	Joseph D. Willson Manager, Interregional Coordination & Compliance	PJM Interconnection, L.L.C. 955 Jefferson Avenue Valley Forge Corporate Center Norristown, Pennsylvania 19403-2497	(610) 666-8820 (610) 666-2296 Fx willsojd@pjm.com
<b>NERC Staff</b>	Craig Lawrence Standards Development Coordinator	North American Electric Reliability Council 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 craig.lawrence@ nerc.net
<b>NERC Staff</b>	Edward H. Ruck Regional Compliance Program Coordinator	North American Electric Reliability Council 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx ed.ruck@nerc.net
<b>NERC Staff Coordinator</b>	Richard Schneider Director of Standards Development	North American Electric Reliability Council 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx richard.schneider@ nerc.net

**Exhibit D**  
**Federal Register Notice**

**UNITED STATES OF AMERICA**  
**Before the**  
**FEDERAL ENERGY REGULATORY COMMISSION**

**NORTH AMERICAN ELECTRIC** )  
**RELIABILITY CORPORATION** )      **Docket No. RR-\_\_\_\_\_**

**NOTICE OF FILING**

Take notice that on March 23, 2007, the North American Electric Reliability Corporation (“NERC”) tendered for filing a request for approval of violation risk factors for NERC’s Version 1 reliability standards pursuant to Section 215 of the Federal Power Act. Specifically, NERC seeks Commission approval for violation risk factors for requirements (i) in Version 1 reliability standards included in the NERC reliability standards approved by the Commission in Order No. 693 issued March 16, 2007, and (ii) in additional Version 1 reliability standards that are pending Commission approval in Docket No. RM06-16 and in other dockets. Upon approval, the proposed violation risk factors will be used to determine penalties or sanctions to be imposed on owners, operators and users of the bulk-power system for violations of the associated requirements in NERC reliability standards.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of the Commission’s Rules of Practice and Procedure (18 CFR 385.211 and 385.214). Protests will be considered by the Commission in determining the appropriate action to be taken, but will not serve to make protestants parties to the proceeding. Any person wishing to become a party must file a notice of intervention or motion to intervene, as appropriate. Such notices, motions, or protests must be filed on or before the comment date. Anyone filing a motion to intervene or protest must serve a copy of that document on the Applicant. On or before the comment date, it is not necessary to serve motions to intervene or protests on persons other than the Applicant.

The Commission encourages electronic submission of protests and interventions in lieu of paper using the “eFiling” link at <http://www.ferc.gov>. Persons unable to file electronically should submit an original and 14 copies of the protest or intervention to the Federal Energy Regulatory Commission, 888 First Street, N.E., Washington, D.C. 20426.

This filing is accessible on-line at <http://www.ferc.gov>, using the “eLibrary” link and is available for review in the Commission’s Public Reference Room in Washington, D.C. There is an “eSubscription” link on the web site that enables subscribers to receive email notification when a document is added to a subscribed docket(s). For assistance with any FERC Online service, please email [FERCOnlineSupport@ferc.gov](mailto:FERCOnlineSupport@ferc.gov), or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Comment Date: \_\_\_\_\_

Magalie R. Salas  
Secretary