126 FERC ¶ 61,065
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Jon Wellinghoff, Acting Chairman;
Suedeen G. Kelly, Marc Spitzer,
and Philip D. Moeller.

Mandatory Reliability Standards for Critical Infrastructure Protection	Docket Nos. RM06-22-002 RM06-22-003

ORDER ON COMPLIANCE FILING

(Issued January 27, 2009)

1. On June 27, 2008, as amended on July 30, 2008, the North American Electric Reliability Corporation (NERC) submitted 12 revised and nine newly-assigned Violation Risk Factors pertaining to certain Critical Infrastructure Protection (CIP) Reliability Standards. In this order, the Commission approves 12 revised Violation Risk Factors and approves nine new Violation Risk Factors as proposed. In addition, the Commission requires revisions to four of the new Violation Risk Factors.

I. Background

2. NERC, the certified Electric Reliability Organization (ERO), is responsible for developing and enforcing mandatory Reliability Standards. As part of its compliance and enforcement program, the ERO uses Violation Risk Factors to delineate the relative risk to the Bulk-Power System associated with the violation of each Requirement or Sub-Requirement element of a Reliability Standard. The ERO assigns a "lower," "medium" or "high" Violation Risk Factor for each element of the mandatory Reliability Standard Requirements,[1] which then becomes a component in determining penalties that the ERO or a Regional Entity assesses for violations of that element. In an earlier order, the Commission established guidelines for evaluating the validity of each Violation Risk Factor assignment.[2]

---

[1] NERC's definitions of high, medium and lower are provided in *North American Electric Reliability Corp.*, 119 FERC ¶ 61,145 at P 9 (*Violation Risk Factor Order*), *order on reh'g*, 120 FERC ¶ 61,145 (2007) (*Violation Risk Factor Rehearing*).

[2] The guidelines are: (1) consistency with the conclusions of the U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004) (Blackout

(continued…)

3. In a March 2007 filing, the ERO submitted initial Violation Risk Factor assignments for all topics of Reliability Standards, including 162 Violation Risk Factors that correspond to Requirement elements of CIP-002-1 through CIP-009-1 (the CIP Reliability Standards). In that proceeding, the Commission addressed the Violation Risk Factors corresponding to Reliability Standards it had already approved. However, at NERC's request, the Commission waited until the instant docket to address the Violation Risk Factors that correspond to the CIP Reliability Standards in order to evaluate them together with the proposed CIP Reliability Standards.[3]

4. On January 18, 2008 the Commission issued Order No. 706,[4] which approved NERC's proposed CIP Reliability Standards and the 162 corresponding Violation Risk Factor assignments that were proposed at that time. In addition, the Commission identified nine Requirements or Sub-Requirements that lacked Violation Risk Factor assignments and directed the ERO to propose assignments. Further, the Commission directed the ERO to revise 43 of the 162 approved CIP Violation Risk Factor assignments. The Commission directed NERC to submit a compliance filing with revised Violation Risk Factors no later than "90 days before the date the relevant CIP Reliability Standards become enforceable."[5] Order No. 706 also directed NERC to develop certain modifications to the CIP Reliability Standards.

II. NERC's Compliance Filings

5. On June 27, 2008, in Docket No. RM06-22-002, NERC submitted a compliance filing that proposes 12 revised Violation Risk Factors pursuant to the Commission directive in Order No. 706. NERC also requests that the Commission waive its

---

Report); (2) consistency within a Reliability Standard; (3) consistency among Reliability Standards; (4) consistency with NERC's definition of the Violation Risk Factor level; and (5) treatment of Requirements that co-mingle more than one obligation. The Commission also explained that this list was not necessarily all-inclusive and that it retained the flexibility to consider additional guidelines in the future. A detailed explanation is provided in *Violation Risk Factor Rehearing*, 120 FERC ¶ 61,145 at P 8-13.

[3] *Violation Risk Factor Order*, 119 FERC ¶ 61,145 at P 14.

[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC ¶ 61,040, *order on reh'g*, 123 FERC ¶ 61,174 (2008).

[5] *Id.* P 757.

regulations and the relevant provisions of Order No. 706 to permit the revised Violation Risk Factors to become effective on July 1, 2008, coinciding with the date that certain CIP Reliability Standard Requirements became enforceable.

6. On July 30, 2008, in Docket No. RM06-22-003, NERC submitted a supplemental compliance filing that includes nine new proposed Violation Risk Factor designations in response to Order No. 706.[6] NERC proposes to assign all nine Violation Risk Factors at the "lower" designation.[7] NERC again requests that the Commission waive its regulations and the relevant provisions of Order No. 706 to permit the nine new Violation Risk Factors to become effective on July 1, 2008.

7. Each of the two filings includes an Exhibit B entitled, "Complete VRF Matrix Encompassing Each Commission approved Reliability Standard."

III. Public Notice

8. Notice of NERC's June 27, 2008 filing, in Docket No. RR06-22-002, was published in the *Federal Register*, 73 Fed. Reg. 42,563 (2008), with interventions or protests due on or before July 28, 2008.

9. Notice of NERC's July 30, 2008 filing, in Docket No. RR06-22-003, was published in the *Federal Register*, 73 Fed. Reg. 45,752 (2008), with interventions or protests due on or before August 19, 2008.

10. No interventions, protests, or comments were filed in response to either filing.

IV. Discussion

A. The 12 Revised Violation Risk Factors (RM06-22-002)

11. The Commission finds that the 12 revised Violation Risk Factors submitted in the filing as amended are modified as directed by the Commission.[8] The Commission therefore approves these 12 Violation Risk Factors, effective July 1, 2008 as requested by NERC.

---

[6] *Id.* P 751, 757.

[7] The July 30 supplemental filing also corrects errata in the initial June 27 filing.

[8] *Id.* P 767.

B. The Nine New Proposed Violation Risk Factors (RM06-22-003)

12. In reviewing the nine new Violation Risk Factor assignments proposed in the July 30, 2008 filing, the Commission used the same guidelines it applied when evaluating the Violation Risk Factor submissions as discussed in the *Violation Risk Factor Order* and Order No. 706. NERC has proposed "lower" Violation Risk Factor assignments for each new Violation Risk Factor. A "lower" risk Requirement, by definition, indicates that the corresponding Requirements are "administrative" in nature.

13. The Commission approves these nine proposed assignments, effective July 1, 2008 as requested by NERC.[9] In addition, the Commission directs NERC to revise four of these Violation Risk Factors. The Commission disagrees with NERC's characterization of these Violation Risk Factor assignments. Specifically, the Commission concludes that the following Sub-Requirements merit a "medium" Violation Risk Factor assignment:

- CIP-003-1, Requirement R4.1 (protection of information about Critical Cyber Assets)
- CIP-005-1, Requirement R1.5 (requiring protective measures for Cyber Assets used in the access control and monitoring of Electronic Security Perimeters)
- CIP-007-1, Requirement R5.1 (authorize access permissions on "need to know" basis)
- CIP-007-1, Requirement R5.3.3 (change password protection at least annually)

The Commission believes that these Sub-Requirements provide significant protections for Cyber Assets and are not simply "administrative." Moreover, pursuant to the Violation Risk Factor analysis guidelines, the Commission believes that a "medium" designation for these four Violation Risk Factors (1) is consistent with the conclusions of the Blackout Report (Guideline 1)[10] and (2) results in more consistency with other Violation Risk Factor assignments in the same or related Reliability Standards. Appendix A to this order identifies the guidelines that the Commission considered in determining that the four Sub-Requirements are more appropriately assigned a "medium" Violation Risk Factor.

---

[9] Specifically, the Commission approves the following proposed Violation Risk Factor assignments: CIP-002-1, R3.1; CIP-003-1, R4.1 and R5.1.2; CIP-004-1, R2.2.2 and R2.2.3; CIP-005-1, R1.5, and CIP-007-1, R5.1, R5.3.3 and R7.

[10] *See* Blackout Report at 163-69, Recommendations 32-44.

14. Accordingly, the Commission approves the nine Violation Risk Factors and directs the ERO to submit a filing containing revisions to four of them, within 60 days of the date of this order. NERC's compliance filing must also include an updated, complete Violation Risk Factor matrix.

The Commission orders:

(A) The 12 revised Violation Risk Factors set forth in NERC's June 27, 2008 compliance filing (Docket No. RM06-22-002) are hereby approved, effective July 1, 2008, as discussed in the body of this order.

(B) The nine Violation Risk Factors set forth in NERC's July 30, 2008 compliance filing (Docket No. RM06-22-003) are hereby approved, effective July 1, 2008, as discussed in the body of this order.

(C) NERC is hereby directed to submit a compliance filing, within 60 days of the date of this order, which includes modifications to four Violation Risk Factors and a complete Violation Risk Factor matrix, as discussed in the body of this order.

By the Commission. Commissioner Kelliher is not participating.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

Appendix A

Standard Number	Requirement Number	Text of Requirement Segment	Violation Risk Factor		Guideline
			NERC Proposal	Commission Determination	
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.	LOWER	MEDIUM	1, 2
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.	LOWER	MEDIUM	1,2,4
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.	LOWER	MEDIUM	2
CIP-007-1	R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.	LOWER	MEDIUM	3

Guideline 1: VRF is not consistent with conclusions of the Final Blackout Report
Guideline 2: VRF is not consistent within a Reliability Standard
Guideline 3: VRF is not consistent among Reliability Standards with similar Requirements
Guideline 4: VRF is not consistent with NERC's Definition of the VRF Level
Guideline 5: Requirement obligation that co-mingles more than one obligation

Document Content(s)