BEFORE THE
ONTARIO ENERGY BOARD
OF THE PROVINCE OF ONTARIO

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION)
)

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF REVISED RELIABILITY STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION AND REVISED IMPLEMENTATION PLANS

Gerry W. Cauley
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
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

January 21, 2010

TABLE OF CONTENTS

ATTACHMENTS:

Exhibit 1: CIP Version 3 Reliability Standards Proposed for Approval.

Exhibit 2: Record of Development of Proposed Reliability Standards.

Exhibit 3: Standard Drafting Team Roster.

Exhibit 4a: Revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities Proposed for Approval

Exhibit 4b: Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3

Exhibit 5: Order No. 706 Directives with Associated Timelines

Exhibit 6a: Proposed Violation Risk Factors and Violation Severity Levels for Modified Version 3 CIP Standard Requirements

Exhibit 6b: Complete Listing of Violation Risk Factors and Violation Severity Levels for Version 3 CIP Standards

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") respectfully submits this filing, which was prepared in response to the Federal Energy Regulatory Commission's ("FERC") Order issued September 30, 2009[1] approving Version 2 of the Critical Infrastructure Protection ("CIP") Reliability Standards ("Version 2 CIP Order"). This filing includes:

1. A request for approval of Version 3 of the Critical Infrastructure Protection Reliability Standards ("Version 3 CIP Standards");[2]
2. A request for approval of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and the Implementation Plan for Version 3 of the Cyber Security Standards CIP-002-3 through CIP-009-3 ("Implementation Plan for Version 3") that addresses FERC's directives in the Version 2 CIP Order; and
3. An update of the timetable that reflects the plan to address the remaining FERC directives from Order No. 706.[3]

The Version 2 CIP Order approved the Version 2 CIP Reliability Standards and the CIP Version 2 Implementation Plan and directed NERC, as the Electric Reliability Organization ("ERO"), to develop certain modifications to the Version 2 CIP Reliability Standards and the associated Version 2 Implementation Plan, and to submit an updated timeline for addressing the remaining Order No. 706 directives. FERC directed NERC to respond to the directives in the Version 2

---

[1] *North American Electric Reliability Corporation*, Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing, 128 FERC ¶ 61,291 (2009) ("Version 2 CIP Order").

[2] Version 3 of the CIP Standards is the same as Version 2 in all respects, except for the specific changes made to CIP-006-2 and CIP-008-2 to address the directives from the Version 2 CIP Order. NERC is resubmitting all CIP standards as Version 3 CIP standards for ease of reference.

[3] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040 (2008) ("Order No. 706").

CIP Order within ninety days, or by December 29, 2009. This filing addresses FERC's directives.

The NERC Board of Trustees approved the Version 3 CIP Reliability Standards, the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and the Implementation Plan for Version 3 on December 16, 2009. NERC requests approval of the proposed Version 3 Reliability Standards, to be made effective in accordance with the effective date provisions set forth in the proposed Reliability Standards. NERC also requests approval of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, to be made effective April 1, 2010, the same date the Version 2 CIP standards become effective.

Exhibit 1 to this filing sets forth the proposed Version 3 CIP Reliability Standards. **Exhibit 2** contains the complete development record of the proposed Reliability Standards. **Exhibit 3** contains the roster of the standard drafting team that developed the proposed Reliability Standards. **Exhibit 4a** contains the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. **Exhibit 4b** contains the Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3. **Exhibit 5** contains an update of the timetable that reflects the plan to address the remaining FERC directives from Order No. 706. **Exhibits 6a** and **6b** provide revisions to the Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") associated with the CIP Version 3 changes, and an updated complete listing of VRFs and VSLs, respectively.

NERC submitted these proposed Reliability Standards and Implementation Plans with FERC on December 29, 2009, and is also filing these proposed Reliability Standards and Implementation Plans with the other applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

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

Gerry W. Cauley
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
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

III. RESPONSES TO VERSION 2 CIP ORDER

A. Version 3 CIP Standards

In the Version 2 CIP Order, FERC directed NERC to modify the Version 2 CIP Standards as follows:

Version 2 CIP Order, P 30:

> Pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop a modification to Reliability Standard CIP-006-2, through the NERC Reliability Standards development process, to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit, within 90 days from the date of this order ...

Version 2 CIP Order, P 38:

> Pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop a modification to Reliability Standard CIP-008-2, Requirement R1.6, through the NERC Reliability Standards development process, to remove the last sentence of CIP-008-2 Requirement R1.6.

In accordance with FERC's directives in Paragraphs 30 and 38 of the Version 2 CIP Order, NERC hereby submits a revised set of Version 3 CIP standards. The modifications to proposed CIP-006-3 and CIP-008-3 were developed using NERC's *Reliability Standards Development Procedure* and were approved by stakeholders through the NERC balloting process. While the modifications proposed in this filing pertain only to CIP-006 and CIP-008, NERC submits the full suite of CIP standards, CIP-002 through CIP-009 as Version 3 for ease of reference and to simplify applicable entities' understanding in determining the appropriate implementation date. In addition, new VRFs and VSLs are proposed for the modified requirements in CIP-006-3 and CIP-008-3. Conforming changes to the VSLs for CIP-005-3 and CIP-007-3 were deemed necessary in converting CIP-002-2 through CIP-009-2 into CIP-002-3 into CIP-009-3. These confirming changes are included in **Exhibit 6a and 6b for approval.** For those requirements not being modified in this filing, NERC requests carrying forward the Version 2 VRFs and VSLs to the Version 3 requirements.

1. Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC *Reliability Standards Development Procedure*, which is incorporated into the Rules of Procedure as Appendix 3A. NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards.

The development process is open to any person or entity with a legitimate interest in the reliability of the bulk power system. NERC considers the comments of all stakeholders and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard before its submission to applicable governmental authorities.

The proposed Reliability Standards set out in **Exhibit 1** have been developed and approved by industry stakeholders using NERC's *Reliability Standards Development Procedure*. They were approved by the NERC Board of Trustees on December 16, 2009.

2. Justification for Approval of Proposed Reliability Standards

In this filing, NERC is proposing Version 3 CIP Standards, which are responsive to FERC's directives in the Version 2 CIP Order. No other changes are being proposed apart from those identified in the Version 2 CIP Order.

3. Summary of Reliability Standards Development Proceedings

Following the issuance of the Version 2 CIP Order, NERC initiated a new project, Project 2009-21 — Cyber Security Ninety-Day Response to address FERC's directives. The Standards Committee assigned the existing Cyber Security Order No. 706 standard drafting team to address the directives in the Version 2 CIP Order. The scope of the project included developing the changes to CIP-006-2 and CIP-008-2 as directed by FERC and developing conforming changes to CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, CIP-007-2, and CIP-009-2 to correct the cross references to CIP-006 and CIP-008 within the set of standards. Additionally, VRFs and VSLs are included for modified requirements in CIP-006-3 and CIP-008-3. The project scope also included revising the CIP Version 2 Implementation Plan to address the matters specified in the Version 2 CIP Order. The Implementation Plan changes are discussed in Section III.B of this filing.

NERC posted the proposed Standards Authorization Request for Project 2009-21, proposed Version 3 CIP standards changes, associated VRFs and VSLs, the proposed Implementation Plan for the Version 3 CIP standards, and a revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for a 30-day industry

comment period that concluded on November 12, 2009. There were 29 sets of comments received in response to the posting from more than 60 people in 40 different companies representing 8 of the 10 Industry Segments. In addition to comments regarding the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to be discussed in the following section, the team determined that changes to CIP-006-3 were necessary to more closely conform to the specific FERC directive.

As a result, whereas CIP-006-2, Requirement R1 requires the applicable entity to document, implement, and maintain a physical security plan that includes, in accordance with sub-requirement R1.6, "[c]ontinuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access," the proposed version of CIP-006-3, sub-requirement R1.6 has been expanded to the following:

> **R1.6** A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
>
> **R1.6.1**. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
>
> **R1.6.2**. Continuous escorted access of visitors within the Physical Security Perimeter.

Additionally, in accordance with FERC's directive, NERC also proposes a revised CIP-008-3 standard that removes the last sentence of sub-requirement R1.6.

> **R1.6.** Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. ~~Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.~~

In order to meet FERC's ninety-day response window, the NERC Standards Committee authorized deviations from the typical standards development process by commencing the pre-ballot review window and assembly of the ballot pool concurrent with the industry comment period. The ballot pool and pre-ballot review window began on October 27, 2009 and concluded

on November 20, 2009. NERC held the initial ballot for the Version 3 CIP Standards, associated VRFs and VSLs, the Implementation Plan for the Version 3 CIP Standards, and the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities from November 20, 2009 through November 30, 2009. With 89.58 percent of the ballot pool participating, the proposed standards and associated documents achieved a weighted segment approval of 88.07 percent. There were 28 negative ballots where 17 comments were submitted with a negative ballot and 5 accompanying an affirmative ballot. No commenters addressed the changes proposed in CIP-008-3. However, several commented on the proposed CIP-006-3 modifications, including one commenter that disagreed with FERC's timeline for delivery of these changes. In the commenter's view, the changes were inconsequential to reliability and diverted scarce resources working on the substantive revisions to the CIP standards, as required by Order No. 706, in order to address FERC's directives in the Version 2 CIP Order.

The team clarified its intent in the response to the various comments but made no changes to the proposed standards as a result. NERC conducted the recirculation ballot from December 3, 2009 through December 14, 2009. With 93.33 percent of the ballot pool voting, the proposed standards and associated documents achieved a weighted segment approval of 85.55 percent. The NERC Board of Trustees approved the standards, VRFs and VSLs, the associated Version 3 CIP Standard Implementation Plan, and a revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities via conference call on December 16, 2009.

B. Revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Version 2 CIP Order, P 40:

> We reject the first document identified above, "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2," because it is unnecessary and causes confusion. For instance, this document discusses the proposed effective date of the Version 2 CIP Reliability Standards, but this discussion is unnecessary because each such Standard includes a provision describing its effective date. The first document also discusses the date by which "newly registered entities" must comply with the Version 2 CIP Reliability Standards. This document does not define "newly registered entities," but its statements appear consistent with the timeline for compliance set forth in Table 3 of the second document that applies to "Entities Registering in 2008 and Thereafter." We believe the first document is confusing since it is unclear how it relates to the second document. If NERC believes that information contained in this document is useful for explanatory purposes, NERC should incorporate the relevant information into the second implementation plan to create a single, comprehensive document.

Version 2 CIP Order, P 41:

> Considered alone, we find that the second document identified above, "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or their Successor Standards," (the Version 2 Implementation Plan or Version 2 plan) lacks clarity and could be open to multiple interpretations on some topics. Commission Staff prepared a document reflecting our concerns in this regard, which is attached to this order. We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order.

First, a brief history of the CIP implementation plans is in order. FERC approved the implementation plan that NERC proposed for Version 1 of the CIP Standards in Order No. 706.[4] That implementation plan provided for implementation of the CIP Version 1 Reliability Standards over a three-year period. It set out a proposed schedule for accomplishing the various tasks associated with compliance with the CIP Reliability Standards and gave a timeline, by

[4] Order No. 706, P 86.

calendar quarters, for completing various tasks and prescribed milestones for when a responsible entity must: (1) "begin work" to be compliant with a requirement; (2) "be substantially compliant" with a Requirement; (3) "be compliant" with a Requirement; and (4) "be auditably compliant" with a Requirement. According to the implementation plan, "auditably compliant" must be achieved in 2009 for certain Requirements by certain responsible entities, and in 2010 for others. The responsible entities were classified as Table 1, Table 2, Table 3, or Table 4 entities, with various implementation dates, depending on which functions they were registered for and whether or not they had previously been required to certify compliance with Urgent Action Cyber Standard 1200. All were to be auditably compliant by December 31, 2010.

When NERC filed Version 2 of the CIP Reliability Standards in May 2009, it also filed a revised implementation plan, in two documents. The first document, styled "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2," stated that when the Version 2 standards became effective, the Version 1 standards and the Version 1 implementation plan would be retired. The first part also repeated the effective date provision from each of the Version 2 CIP standards, namely, that the Version 2 standards become effective "on the first day of the third quarter after receiving regulatory approval." The Version 2 implementation plan also stated that responsible entities must comply with the Version 2 CIP standards "once the standards become effective."

The second document filed in May 2009 was styled "Implementation Plan for Newly Identified Critical Cyber Assets or Newly Registered Entities for Cyber Security Standards CIP-003-1 through CIP-009-1 or Their Successor Standards." The purpose of the second document was to specify an implementation schedule for situations where an entity already subject to the CIP standards identified new critical cyber assets or where an entity was newly included on the

NERC Compliance Registry (and thus was subject to CIP standards for the first time, specifically CIP-002 that required the use of a risk-based methodology for identifying Critical Cyber Assets).

In the Version 2 CIP Order, FERC rejected the first document as unnecessary, because it repeated the effective date provisions from each of the Version 2 CIP standards. NERC understands the effect of the Version 2 CIP Order in this regard is that responsible entities must be in compliance with Version 2 of the CIP standards as of April 1, 2010, the date those standards become effective. FERC found that the second document lacked clarity in several aspects and directed NERC to file a revised document that addressed the issues listed.

The revised Implementation Plan called for by the Version 2 CIP Order is presented in two documents in this filing. The first document, **Attachment 4a**, is styled "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities." It applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3. This document addresses the enumerated list of corrections and clarifications that were included with FERC's Version 2 CIP Order. NERC requests approval of this implementation plan, to be made effective on April 1, 2010, to coincide with the effective date of the CIP Version 2 standards.

The second document, styled as "Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3" (**Attachment 4b**), does a number of things, all in one place. First, it states that prior versions of the CIP standards will be retired when the Version 3 CIP standards become effective. Second, it states that responsible entities must be compliant with Version 3 of the CIP standards on the date those standards become effective. Third, the document references the effective date provision in the Version 3 CIP standards, which states that the Version 3 CIP standards become effective on the first day of the third quarter following regulatory approval. By way of example, if a governmental authority approves the Version 3

CIP standards before April 1, 2010, then the Version 3 CIP standards will become effective October 1, 2010. Responsible entities would then be required to be in compliance with the Version 3 CIP standards as of that date.[5] Fourth, the document explains that Newly Identified Critical Cyber Assets and Newly Registered Entities are covered by the "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities." Finally, the second document explains that the original implementation plan for the Version 1 CIP standards will, as a practical matter, end on December 31, 2010, because on that date all Table 1, 2, and 3 entities must be auditably compliant.

As of April 1, 2010, NERC envisions two Implementation Plans will be in effect – the Implementation Plan for Version 3, which effectively implements the Version 1 implementation plan dates for Table 1, Table 2, and Table 3 entities for Version 1, Version 2, or Version 3 standards, whichever are in effect; as well as the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. On December 31, 2010, when the Version 1 Implementation Plan implementation dates are, in practice, retired, only the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities will remain in effect.

While FERC expressed concern over the usefulness of the Version 2 Implementation Plan document and directed that NERC incorporate the relevant information into the second document, NERC believes each document serves a useful purpose. Therefore, NERC chose to clarify the content of each document to remove the confusion noted in FERC's attachment to the Version 2 CIP Order. In addition to defining "newly registered entities," FERC identifies a list of 13 concerns in the attachment, designated "a" through "m," which NERC addresses in

[5] It is important to note that the only substantive changes from Version 2 to Version 3 occur in CIP-006 and CIP-008, in response to directives in the Version 2 CIP Order.

sequential order below. Following this discussion, a description of the development activities relative to the implementation plans is provided.

a. The Version 2 Implementation Plan states at page 1 that it identifies the schedule for becoming compliant with the requirements of CIP-003-2 through CIP-009-2 and their successor Standards "for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed." The use of the phrase "existing Implementation Plan" here and elsewhere on page 1 of the Version 2 Implementation Plan causes confusion as to whether the Version 1 Implementation Plan or the proposed plan is being referenced. We direct NERC to clarify that the "existing" implementation plan is the Version 1 Implementation Plan.

The reference to "existing Implementation Plan" has been clarified in the proposed revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. In the second paragraph on Page 1, NERC clarifies that the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities applies to Version 2 or Version 3 of the CIP standards for both: a) newly identified Critical Cyber Assets by existing Registered Entities after their Compliant milestone date has passed; and, b) newly Registered Entities, thus addressing two distinct scenarios for different types of entities.

The first scenario concerns entities that are already registered on the NERC Compliance Registry, and are therefore subject to compliance with NERC Reliability Standards. It is therefore assumed that these entities are already compliant with the requirements of CIP-002, have a risk-based methodology for identifying Critical Assets, and have identified any Critical Cyber Assets associated with the identified Critical Assets. In this scenario, newly identified Critical Assets and/or newly identified Critical Cyber Assets are designated as a result of the application of the risk-based methodology in CIP-002, and as described in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. In this scenario, the entity must follow the timeline defined in Table 2 of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to determine when it must be

compliant with the requirements of CIP-003 through CIP-009.

The second scenario deals with a wholly new registered entity that has no history of registration on the NERC Compliance Registry under its existing or predecessor organization, and therefore has not previously been required to be compliant with the NERC Reliability Standards. Note that merged and acquired companies, and acquired assets are specifically discussed in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the context of the first scenario described in the previous paragraph.

When the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was originally submitted with the Version 2 CIP standards, there was no way of determining what the specific compliance dates for Version 2 would be, thus there was no specificity with regard to the compliance dates. Version 1 and Version 2 implementation dates are now known, and have been included in the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. In order for the proposed Implementation Plan dates for Newly Identified Critical Cyber Assets and Newly Registered Entities to coincide with the April 1, 2010 effective date for Version 2 of the CIP standards, NERC requests approval of this Implementation Plan to become effective on April 1, 2010.

b. The Version 2 Implementation Plan refers at page 3 several times to "this New Asset Implementation Plan." We direct NERC to delete or change this inaccurate reference.

NERC adds significantly more specificity to the various categories and milestones in the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities such that the objectionable term, "New Asset Implementation Plan" is not necessary and is deleted in the proposal included in this filing.

c. The Version 2 Implementation Plan refers at pages 3 and 4 several times to "an established CIP Compliance program as required by an existing Implementation Schedule." We direct NERC to clarify the meaning of "an established CIP Compliance program." In particular, we direct NERC to state whether a "CIP Compliance program" includes a program for complying with CIP-002 or is limited to a CIP compliance program for CIP-003 through CIP-009, as stated for Category 1 listed under the heading "Implementation Schedule" on page 1 of the Version 2 Implementation Plan. We also direct NERC to clarify the meaning of "an existing Implementation Schedule."

In footnote 3 on Page 2 of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, NERC clarifies the term "CIP compliance implementation program" to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC CIP Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All existing Registered Entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version-specific Implementation Plan. NERC clarifies that the applicable milestones for various categories of Registered Entities are governed by Tables 1, 2, and 3 of the CIP Version 1 standard implementation schedules. The Version 1 Implementation Plan therefore provides the applicable implementation dates for Table 1, Table 2, and Table 3 entities. This is described in more detail in the Implementation Plan for Version 3, included in **Exhibit 4b** to this filing.

The Version 2 CIP Order has set the implementation date for Version 2 of the CIP standards as April 1, 2010. For entities that registered on the NERC Compliance Registry after April 2008, the implementation schedule for the Version 2 or Version 3 CIP standards, whichever are in effect, can be determined through Table 3 of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. Accordingly, NERC requests approval of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities effective April 1, 2010, to coincide with the effective date of the CIP Version 2 standards.

To further add clarity to the implementation and enforcement schedules relative to Versions 1 and Version 2, NERC intends to update its 2010 Uniform Compliance Monitoring and Enforcement Program ("CMEP") Implementation Plan to account for the "effective date" of the Version 2 CIP standards of April 1, 2010 for all entities. When a compliance audit occurs, the Responsible Entity will be audited to the Version 1 CIP standards for the portion of the audit period prior to April 1, 2010 and to Version 2 for the remainder of the audit period after April 1, 2010. However, the compliance milestones (the "compliant" and "auditably compliant" dates) will remain set by the original Version 1 implementation plan: for Table 1 entities, the auditably compliant date is July 1, 2009 for 13 requirements and July 1, 2010 for the remaining requirements; for Table 2 entities, the auditably compliant date is July 1, 2009 for CIP-003, Requirement R2 and July 1, 2010 for all remaining requirements; and for Table 3 entities the auditably compliant date is December 31, 2009 for CIP-003, Requirement R2 and December 31, 2010 for all remaining requirements. In effect, the April 1, 2010 effective date determines the substance of the audits, but the original Version 1 Implementation Plan will continue to set the schedule for the audits.

d. We direct NERC to clarify whether the Version 2 Implementation Plan contemplates that the Version 1 Implementation Plan will be retired upon the effective date of the Version 2 CIP Reliability Standards. If not, we require further explanation as to how the Version 1 Implementation Plan will still be applicable. The revised plan should be clear which entities must continue to rely upon the Version 1 Implementation Plan, and to what extent in which circumstances.

NERC includes in this filing the Implementation Plan for Version 3, which explains that the implementation dates included in Version 1 of the Implementation Plan shall remain in effect for Table 1, Table 2, and Table 3 entities for compliance with Version 1, Version 2, and Version 3, whichever is in effect, until the implementation dates are in practice, retired on December 31, 2010. The last section of this document entitled, "Prior Version Implementation Plan

Retirement," includes specific detail regarding the retirement of the Version 1 Implementation Plan Tables 1, 2, and 3 and concludes that as of December 31, 2010, the date on which Table 3 Registered Entities reach the Auditably Compliant state, the Version 1 Implementation Plan is no longer needed and will be retired. This aspect is also consistent with the process noted above that will be updated in the 2010 CMEP Implementation Plan. Table 4 of the Version 1 Implementation Plan deals with the treatment of newly Registered Entities. These entities are wholly included in Table 3 of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, submitted with this filing, that NERC is requesting approval, to be made effective on April 1, 2010. After December 31, 2010, the only Implementation Plan in effect will be the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities submitted with this filing.

e. In the third paragraph of page 1, the Version 2 Implementation Plan refers to "some requirements" for which a Responsible Entity is expected to be Compliant upon the designation of the newly identified Critical Cyber Asset, stating that these instances are "annotated as '0'." We observe that the Version 2 Implementation Plan does not annotate any requirement as "0." We direct NERC to explain or delete this statement and to list each requirement for which a Responsible Entity is expected to be Compliant immediately upon designation of a newly identified Critical Cyber Asset.

NERC has deleted the incorrect annotation and has further described with greater specificity the compliance expectations for newly identified Critical Cyber Assets based on the various categories for identification. Table 1 provides a useful list of examples describing how to apply Table 2 for the various identification scenarios. Generally, there are no requirements in Table 2 for which a Responsible Entity is expected to be Compliant immediately upon designation of a newly identified Critical Cyber Asset. However, for a Responsible Entity with an existing CIP compliance implementation program for CIP-003 through CIP-009, the following conditions require compliance upon the commissioning of the asset:

- any asset identified as a Critical Asset with associated Critical Cyber Assets that comes on-line
- any existing Cyber Asset that is reconfigured to be within the Electronic Security Perimeter
- any new Cyber Asset added into a new or existing Electronic Security Perimeter
- any new Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter, or
- any planned modification or upgrade to an existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset.

f. In the third paragraph of page 1, the Version 2 Implementation Plan also refers to "other requirements" for which the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date, stating that these are annotated as "existing." We observe that Table 2 of the Version 2 Implementation Plan annotates the following requirements as "existing" for "Milestone Category 2": CIP-003-2, R1 through R3 and CIP-004-2 Requirement R1. We direct NERC to confirm whether these requirements are the only requirements annotated as "existing" in the Version 2 Implementation Plan and, if not, to list each other requirement for which the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date.

NERC confirms that the requirements identified by FERC are the only requirements annotated as "existing" in Table 2 of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. Recall that Table 2 assumes the Registered Entity has undergone at least one iteration of the Critical Asset identification process as required by CIP-002.

g. At page 1, under the heading "Implementation Schedule," the Version 2 Implementation Plan lists three categories. Category 2 refers to "An existing Cyber Asset becomes subject to CIP Reliability Standards, *not due to planned change*," while Category 3 refers to "A new or existing Cyber Asset becomes subject to CIP Reliability Standards *due to planned change*" (emphasis in original). We direct NERC to clarify, for purposes of these categories, the meaning of the statement "Cyber Asset becomes subject to CIP Standards." We note that pursuant to CIP-002-2 Requirement R3, a Responsible Entity must consider which of its Cyber Assets are Critical Cyber Assets essential to the operation of a Critical Asset. In that sense, all of a Responsible Entity's Cyber Assets become subject to CIP Reliability Standards when the entity undertakes to comply with CIP-002-2 Requirement R3. We also observe that at page 2, the Version 2 Implementation Plan states that the term "Cyber Asset becomes subject to the CIP standards" applies to "all Critical Cyber Assets, as well as to other (non-critical) Cyber Assets within an Electronic Security Perimeter." However, this statement does not make clear whether NERC intends that formula to be the definition of the term. We direct NERC to clarify the meaning of the term "planned change" that appears in the

description of both categories, because the Version 2 Implementation Plan does not define that term.

NERC understands FERC's directive with respect to the application of CIP-002 for all Cyber Assets and clarifies that the term "Cyber Asset becomes subject to CIP standards" in the revised plan should be modified to read: "Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009." This language applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

NERC also clarifies in the Implementation Milestone Categories section of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities that a "planned change" refers to any changes of the electric system or Cyber Assets that were planned and implemented by the Registered Entity. This contrasts with an unplanned change to the electric system that occurs through the actions of others apart from the Registered Entity. The unplanned change causes the reclassification of a Cyber Asset previously designated not to be a Critical Cyber Asset as a Critical Cyber Asset during the annual application of the CIP-002 process.

h. At page 3, the Version 2 Implementation Plan states that Category 2 applies "only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are ***identified***, not when they are added or modified through construction, upgrade or replacement" (emphasis in original). We direct NERC to clarify this statement because of our concern that it provides an unintended incentive for Responsible Entities to delay identification of assets that trigger the implementation timelines set forth in Table 2. For example, in January 2010 a Responsible Entity could obtain information indicating that an asset already in service should be identified as a Critical Cyber Asset. However, if the Responsible Entity does not so "identify" the asset until December 2010, the period the Version 2 Implementation Plan allows for becoming compliant would begin as much as 11 months later than if the Responsible Entity identified the asset as a Critical Cyber Asset immediately after obtaining information indicating that the asset should be so identified. We note that CIP-002-2 Requirement R3 states that a Responsible Entity shall review its list of Critical Cyber Assets "at least annually, and update it as necessary."

NERC would expect an entity to review its Critical Cyber Assets list "at least annually, and update it as necessary." In the course of a compliance audit, ERO auditors would expect to see evidence demonstrating both (1) that the audited entity had reevaluated its Critical Cyber Assets list each year during the audit period, and (2) that the audited entity incorporated newly identified Critical Cyber Assets into the list during appropriate times between such reviews. In all cases, regardless of the compliance monitoring method, NERC and Regional Entity staff will review whether an entity complied with the re-evaluation element of CIP-002-2, Requirement R3 whenever they identified a Critical Cyber Asset that was not previously on the list of Critical Cyber Assets. Note that if an in-service Critical Cyber Asset is modified or a Cyber Asset is added through construction, upgrade, or replacement by the Responsible Entity, the category "Compliant upon Commissioning" would apply. Therefore, the issue focuses on the identification of other Cyber Assets caused by an unplanned change.

i. Also at page 3, with respect to a business merger where all parties have identified Critical Cyber Assets and have "existing but different" CIP compliance plans in place, the Version 2 Implementation Plan provides that the merged Responsible Entity has one calendar year from the merger's effective date to determine either to combine the programs or operate them separately under a common Senior Manager. The Version 2 Implementation Plan further states that at the conclusion of the calendar year, the merged Responsible Entity will use the Category 2 milestones to consolidate the separate programs. We direct NERC to specify the minimum extent of difference between the compliance plans that would trigger this provision of the Version 2 plan, because, absent this specificity, any difference between the compliance plans could activate this provision. We further direct NERC to explain whether this provision would extend the time period for compliance with applicable Version 2 requirements for the merged Responsible Entity if it (a) did not identify any additional Critical Cyber Assets after the effective date of the merger; or (b) did identify such additional assets.

NERC explains its discourse in Scenario 3 of the revised plan, that any difference, including a simple difference such as the use of different anti-virus software between the two Registered Entities would trigger the provision. With respect to FERC's question pertaining to the extension of time for compliance with the standards following the one-year analysis period,

NERC notes that the compliance programs would be expected to continue for any previously identified Critical Cyber Assets until the combined plan is fully implemented; any newly identified Critical Cyber Assets would be subject to the compliance schedule in Table 2 of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities starting on the date of their identification. Thus, the entity remains subject to compliance with CIP standards during the transition period. Both of these provisions will be subject to review in a CIP Spot Check or Audit

j. At the last paragraph of page 4, the Version 2 plan states, "Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards." The Commission observes that the third sentence is not accurate if the phrase "these standards" is interpreted to include CIP-002-2. We direct NERC to revise this sentence to clarify its meaning.

NERC has revised the referenced language to specify that "[o]nly upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009."

k. We direct NERC to clarify whether the abbreviations used in Table 3 of the Version 2 Implementation Plan (BW, SC, C and AC) have the same meaning as the counterpart abbreviations in the Version 1 plan.

NERC has revised the Table 3 classifications in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for newly registered entities after April, 2008 to only include a "Compliant date" to be consistent with the term used elsewhere in the plan, NERC recognizes the continued relevance of the Compliant and Auditably Compliant designations until the retirement of the Version 1 implementation plan as discussed in item (c). However, when the Version 1 implementation plan dates are retired (*i.e.* on December 31, 2010), the terms used in that document (BW, SC, C, and AC) will no longer be used. The Compliant

dates specified in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities are consistent with those specified in Table 4 of the original Version 1 Implementation Plan.

l. We observe generally that further clarification on the treatment of mergers and acquisitions at pages 3 and 4 of the Version 2 Implementation Plan is appropriate and perhaps could be achieved with explanatory text and examples in an introductory section. The Commission believes that it would be helpful to entities and promote uniform understanding if introductory explanations and/or diagrams were to address the following merger-specific instances: (1) a merger of two or more entities where none have identified a Critical Cyber Asset; (2) a merger of two or more entities where one has identified at least one Critical Cyber Asset; and (3) a merger of two or more entities where each has identified at least one Critical Cyber Asset.

NERC has significantly expanded the discussion in the plan to specifically address each of the scenarios described by FERC for newly Registered Entities based on mergers and acquisitions.

m. We also observe that one or more existing Responsible Entities that have identified at least one Critical Cyber Asset could form a new entity that heretofore has not been registered on the NERC Compliance Registry. Upon the new entity's registration, it could be argued that Table 3 of the Version 2 Implementation Plan would apply to it because it would be an entity "registering in 2008 and thereafter." Interpreted literally, Table 3 then would exempt the newly registered entity from compliance with CIP-003-2 Requirement R2 for 12 months after registration and with the remainder of the requirements of the Version 2 CIP Reliability Standards for 24 months after registration. We direct NERC to explain how it would address this situation in the context of Version 2 implementation. More broadly, because innumerable permutations of merger and acquisition scenarios exist, we direct NERC to incorporate into the Version 2 Implementation Plan explicit language to preclude unfair delay of compliance due to the structure of particular transactions.

NERC specifically addresses the situation noted in FERC's directive by noting in the introduction that the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002, and have existing risk-based Critical Asset identification methodologies. More specifically, in Scenario 2, the merged Registered Entity will implement the CIP compliance implementation program of the predecessor Registered Entity with an identified Critical Cyber Asset, which will be expected to apply to any Critical

Cyber Assets identified after the date of the merger. In this regard, Table 2 will apply, not Table 3 that deals with newly Registered Entities registered in April 2008 or thereafter. Similarly, under Scenario 3 that deals with predecessor Registered Entities where each has identified at least one or more Critical Cyber Asset, the language in sub-section (a) indicates that any new Critical Cyber Assets identified as a result of a merged Critical Asset identification methodology will be treated as a newly identified Critical Cyber Assets and fall under Table 2 as a result. Until such time that the methodologies are combined, the predecessor programs and methodologies will be applied, and any newly identified Critical Cyber Assets will be treated under Table 2 as well.

In summary, if an entity falls within scenarios 2 and 3 of the merger and acquisitions section that assumes a predecessor Registered Entity has previously identified at least one Critical Cyber Asset, the existing CIP compliance implementation program(s) will carry forward to the merged Registered Entity until such time a decision is made to combine the programs. Whether or not a decision to combine the programs is made, the outcome is the same: Table 2 will apply and any newly identified Critical Cyber Assets will be implemented according to the milestones therein. Table 3 only applies to newly Registered Entities that have not previously applied the CIP-002 Critical Asset identification methodology.

C. Updated Timeline for Addressing Order No. 706 Directives

Version 2 CIP Order, P 43-44:

> 43. In Order No. 706, we directed NERC to develop a timetable as well as submit a work plan for developing and filing for approval the modifications directed by the Commission to the CIP Reliability Standards.[] While we do not object to NERC's multi-phased approach, NERC should provide more information regarding the status of these modifications, such as the inclusion of lessons learned,[] the clarification that Responsible Entities cannot except themselves from the CIP Reliability Standards,[] and identification of the core training elements and parameters for exceptional circumstances.[]

44. We direct NERC to submit as part of the compliance filing required by this order an update of the timetable that reflects the plan to address remaining Commission directives from Order No. 706. The filing should be a report of current status, addressing all of the projects including those that are underway and already planned as well as those that have been deferred or not yet scheduled, with a summary description of which Order No. 706 directives NERC plans to address during each phase.

NERC has developed an approach to addressing the directives in Order No. 706 that reflects the importance of expeditiously improving the quality of the currently effective Version 1 CIP standards, and significantly increasing the emphasis of critical infrastructure protection of the bulk power system in general. Principally, these efforts resulted in the establishment of a NERC Critical Infrastructure Protection program in 2008. The primary purpose of this program is to coordinate all of NERC's efforts to improve physical and cyber security for the bulk power system of North America, as it relates to reliability. These efforts include standards development, compliance enforcement, assessments of risk and preparedness, disseminating critical information via alerts to industry, and raising awareness of key issues. Additionally, the program is home to the Electricity Sector Information Sharing and Analysis Center (or ES-ISAC) which monitors the bulk power system to provide real-time situation awareness leadership and coordination services to the electric industry. In addition, NERC's Critical Infrastructure Protection Committee ("CIPC") supports and provides technical subject matter expertise to both programs. The CIPC Executive Committee, along with the President and CEO of NERC, serve as the Electricity Sector Coordinating Council to collaborate with the U.S. Department of Energy ("DOE") and U.S. Department of Homeland Security ("DHS") on critical infrastructure and security matters. The DOE designated NERC as the electricity sector coordinator for critical infrastructure protection. NERC serves as the Information Sharing and Analysis Center for the electricity sector. NERC also works closely with the DHS and Public

Safety Canada to ensure the critical infrastructure protection functions are coordinated with the governments of the United States and Canada.

NERC's increased focus on critical infrastructure protection has manifested itself in a number of important activities, not the least of which is oversight and improvement to the set of Version 1 CIP Reliability Standards as directed in Order No. 706. The timeline for implementing the directives in Order No. 706 is discussed later in this section. Since the formal establishment of the NERC CIP program in July 2008, NERC has:

- Hired a Vice President and Chief Security Officer;
- Developed and delivered compliance auditor training for the Version 1 CIP Reliability Standards;
- Developed and filed the Technical Feasibility Exception process for Version 1 and future CIP Reliability Standards;
- Conducted a High Impact Low Frequency Workshop to engage industry and U.S. government leaders on appropriate actions to consider in addressing this threat;
- Conducted a primary and supplemental survey of entities under compliance with CIP-002-1 to determine how Registered Entities are applying methodologies to identify Critical Cyber Assets;
- Coordinated with the CIPC to develop guidance documents to support Critical Asset identification per CIP-002-1, Critical Cyber Asset identification that is currently in process;
- Issued six advisories in 2009 that directly address Cyber Assets (a subset of CIP), issued three advisories in 2009 that address CIP in general (H1N1 advisories), and issued three Recommendations addressing cyber assets in 2008;
- Continues to support through active participation and through comment opportunities the advancement and integration of SmartGrid equipment on the grid;
- Proposed two updated versions of CIP Reliability Standards based on directives issued in Order No. 706 and in the Version 2 CIP Order, while pursuing more substantive changes to the CIP reliability standards based on the remaining Order No. 706 directives;
- Established the North American Synchro-Phasor Initiative;
- Filed an Implementation Plan for U.S. nuclear power plants relative to NERC's Version 1 CIP Reliability Standards;
- Coordinated with the Nuclear Regulatory Commission on the development of a memorandum of understanding regarding implementation of critical infrastructure protection at U.S. nuclear power plants; and

- Filed numerous standards interpretations to Version 1 CIP Reliability Standards.

This compendium of critical infrastructure activities demonstrates NERC's and the industry's commitment to improving critical infrastructure protection for the bulk power system and preserving reliability. At the core of these activities, however, is the establishment of a set of mandatory and enforceable Reliability Standards that Registered Entities are obligated to implement for their Cyber Assets relating to the bulk power system. NERC submitted in August, 2006 and FERC approved in January 2008 an initial set of CIP Reliability Standards, referred to as the Version 1 CIP standards. While noting that these standards serve a useful reliability purpose, they establish the minimum set of expectations and require significant improvement to achieve the level of ultimate acceptability to protect the bulk power system.

Accordingly, FERC identified a lengthy list of improvements through directives set forth in Order No. 706 for NERC to address. Some of the directives require changes to the standards themselves, requiring industry stakeholders to develop and approve these changes through the *Reliability Standards Development Procedure*. Other directives regarding guidance in implementing the existing CIP standards were assigned to NERC's Critical Infrastructure Protection Committee to develop or are awaiting further refinement to the requirements before developing the needed guidance. For directives requiring standards changes, NERC, working through its industry drafting team and the Standards Committee, elected to apportion these improvements in a multi-phase approach. Each phase would result in a separate filing, representing a new version of the standards. The first phase of this improvement project that resulted in the Version 2 CIP standards addressed the following items that were of significance to FERC in its Order No. 706 and other non-controversial items the team believed would receive industry acceptance:

- removal of the term "reasonable business judgment" from the purpose section of each Reliability Standard;

- removal of the term "acceptance of risk" from each Reliability Standard;

- specification in CIP-002-2 Requirement R4 that the senior manager must annually approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets;

- requirement in the CIP-003-2 Applicability section that all Responsible Entities must comply with CIP-003-2 Requirement R2;

- specification in CIP-003-2 Requirement R2 that a single manager with overall responsibility and authority must be designated;

- specification in CIP-003-2 Requirement R2.3 that delegations of authority must be documented;

- specification in CIP-004-2 Requirement R2 that all employees with authorized access must be trained prior to access, except in specified circumstances;

- clarification in CIP-004-2 Requirement R3 that the Responsible Entity shall have a documented personnel risk assessment program, prior to personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets;

- clarification in CIP-006-2 Requirement R1 that the Responsible Entity shall document, implement and maintain a physical security plan, approved by the senior manager; and

- identification of a Responsible Entity's compliance schedule in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

NERC filed a request for approval of these standards on May 27, 2009. Additional revisions to the Version 2 standards directed by FERC in its Version 2 CIP Order are presented as Version 3 CIP standards in this filing. In order to meet the FERC ninety-day delivery timeframe for the Version 3 CIP standards, the NERC drafting team received approval from the Standards Committee to use a modified development process that slightly differs from that customarily used and currently approved in NERC's Rules of Procedure, Appendix 3A.

NERC has outlined an updated plan in **Exhibit 5** to this filing to address the remaining directives originating from Order No. 706. For completeness, **Exhibit 5** includes all directives

from the Order. For each item in the list, NERC includes a description of its current status and the version of the development activity in which the item has been or will be addressed. NERC intends to address the remaining activities in future submissions.

NERC also acknowledges various items that NERC was directed to *consider* in Order No. 706. To the extent the issues for consideration are appropriate for consideration during the Version 4 activities described below (*i.e.,* activities specifically focused on FERC's directives in Order No. 706), the team will consider the items. Otherwise, the team will consider the items in future development activities.

In order to improve consistency in identifying Critical Cyber Assets based on the experiences in applying the current CIP-002-1 standard requirements, NERC will first propose a revised CIP-002 standard that includes a significant paradigm shift in the approach relative to the current mandatory expectations. This change in approach was conceptually outlined in the drafting team's concept paper, *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions* that was presented for industry review and comment in July 2009. The proposed methodology proposes a mapping of Bulk Electric System ("BES") subsystems into categories based on their impact on the reliability or operability of the BES. The drafting team posted the first draft of CIP-002-4 for an informal industry comment period on December 29, 2009. Using the NERC Standards Development Process, this Version 4 activity and delivery of a revised CIP-002-4 standard is expected to be completed in May 2010. NERC will advise FERC if there should be a significant change in this schedule.

The next significant portion of work, noted as the second part of Version 4, is the development of a suite of security requirements (controls) for each of the impact categories identified in CIP-002-4 for each BES subsystem, identified as generation, transmission, and

control centers. These requirements are intended to modify, replace, retire, and in some cases, add to the current CIP-003 through CIP-009 standard requirements. The body of work associated with the second part of Version 4 represents the most significant volume of work remaining and includes many of the Order No. 706 directives not yet addressed. NERC's current plan is to file the updated versions of CIP-003 through CIP-009 by year-end 2010.

The remaining activities, identified as post Version 4, represent the subset of directives and considerations from Order No. 706 that NERC believes will require significantly more time to discuss and develop the appropriate technical solutions. NERC will begin working on these post-Version 4 modifications once the Version 4 standards are filed with the applicable governmental authorities. At that time, a schedule for those activities will be developed. The key post-Version 4 activities are:

- defense in depth approaches for electronic and physical security perimeter (Order No. 706, PP 496, 502, 503, 572, 575);
- vulnerability assessments (Order No. 706, PP 547, 643) and operational exercises for recovery (Order No. 706, P 725); and,
- forensics (Order No. 706, PP 706, 710).

While NERC understands the obligation to address these directives, NERC also believes there needs to be a more thoughtful and deliberate technical discussion on the approach used to address these items due to the potential detrimental impacts to reliability or extraordinary costs to implementation that could result with a literal implementation of the directives. NERC believes it prudent to engage FERC staff and industry technical experts to develop an approach to these directives that achieve the intended outcome — to protect and preserve the reliability of the Bulk Power System — while not introducing adverse reliability outcomes or exorbitant costs to implement.

NERC notes that the concepts contained in these directives are complex, and will require extensive debate, discussion, research, and in at least one case, vendor research and development before a set of mandatory and enforceable requirements can be drafted that will allow compliance by all applicable entities on all applicable systems. NERC does not believe that this can be accomplished in the timeframe proposed for the Version 4 changes. NERC also notes that there will be significant departure from the current standards methodology of protecting Critical Cyber Assets, moving to an approach where all BES Cyber Systems are protected, which is a significant increase in the scope of applicability for the CIP standards. Given this increase in current scope, NERC does not believe that these four areas can be properly addressed in the proposed timeframe for Version 4.

With respect to the defense in depth approaches for electronic and physical security perimeters, NERC notes that there is need for extensive debate and discussion within the industry on exactly how to accomplish the directives noted in Order No. 706. If taken literally, the defense in depth principle would seem to require two independent methods of either physical or electronic security surrounding a protected asset (even though the Order indicates that this literal interpretation is not intended). While this is practical and achievable in a control center or data center environment, it is problematic in substation or generating plant environments. As discussed in NERC's filing in response to the FERC Notice of Proposed Rulemaking ("NOPR"),[6] there are also safety and performance issues related to multiple layers of defense in depth.

FERC also notes that entities may wish to rely on Technical Feasibility Exceptions when claiming that multiple layers of defense in depth are not practical. However in its development

[6] *See* NERC's October 5, 2007 filing in response to Notice of Proposed Rulemaking ("NERC's Filing in Response to NOPR"), Section J.

of future versions of the CIP standards, the drafting team is attempting to reduce the necessity and reliance on technical feasibility exceptions, based on input from NERC, the Regional Entities, and the industry. Careful wording of the requirements is therefore necessary in order to reduce continued reliance on Technical Feasibility Exceptions, thereby streamlining the audit process, and more directly communicating mandatory and enforceable requirements to the stakeholders.

With respect to vulnerability assessments and operational exercises for recovery, NERC notes that the performance of vulnerability assessments on live operations is challenging, and if done improperly, can be detrimental to the reliable operation of the systems, and therefore detrimental to reliable operation of the bulk power system.[7] NERC acknowledges that a vulnerability assessment should be performed against the systems employed in the bulk power system, but entities must work closely with their technology providers to develop safe test procedures for assessments on *live* systems or develop approaches to perform testing in a test environment that closely replicates the live system. In many cases, particularly with legacy systems or for custom built systems of which there is only a single copy, full test environments cannot be made available for performing vulnerability tests or recovery exercises. In these cases, it is possible that hardware and software are no longer manufactured, and cannot be purchased for such purpose, and the redundant systems deployed for availability of critical functions (*e.g.*, a primary-reserve control system) cannot be sufficiently decoupled to allow full vulnerability testing or recovery exercises of the system without impacting the live system.

NERC is working with entities on a voluntary basis to further explore how to best design and develop cyber focused operational exercises for system recovery. NERC's Critical Infrastructure Protection program has engaged both registered entities and government

[7] *See* NERC's Filing in Response to NOPR, Section K.

stakeholders to conduct a series of table top exercises, such as Secure Grid 2009 and several Cyber Risk Preparedness Assessments, to advance the development of recovery exercises that are driven by cyber induced outages. The work to date has demonstrated the value of developing cyber scenarios to drive recovery exercises. NERC will continue to work with stakeholders to provide guidance and examples for the development of cyber-based recovery exercises.

NERC also believes that some aspects of the directives are better suited to be included in guidance documents, which can be developed once the revised requirements are complete.

With respect to forensics, NERC notes that the term "forensics" connotes specific methods of handling data as evidence, including "chain of custody" and protection of data during analysis.[8] NERC believes that data analysis associated with failures and misuse of systems is important, but is not currently feasible for a large portion of the installed technology that is important to the operation of the bulk power system. Many field devices (*e.g.*, relays in use at transmission substations) do not currently have rapid data extraction techniques available or, in many cases, sufficient security logging, that facilitate the extraction of operational and investigative data in the field while continuing to operate. Research and development by equipment vendors will be needed in order to produce equipment that is capable of rapid unobtrusive data extraction. NERC is involved in both the DHS Control Systems Security Program and the DOE National Supervisory Control and Data Acquisition ("SCADA") Test Bed to support continued advancement of security response and forensics capabilities and tools for electric infrastructure systems. At the point where sufficient advancements are made, the

[8] *See* NERC's Filing in Response to NOPR, Section L

developed equipment will need to be purchased and installed in the field before specific data extraction requirements can be made mandatory and enforceable.[9]

Finally, NERC points out that because of the paradigm shift in the approach for its critical infrastructure protection standards to provide protection for all BES cyber systems, beginning with CIP-002-4, several of the directives and considerations in Order No. 706 are rendered meaningless. Therefore, FERC's concerns will have been ameliorated by virtue of the shift in philosophical approach to categorizing cyber systems based on the BES subsystem impact mapping.

V. CONCLUSION

The North American Electric Reliability Corporation respectfully requests approval of this filing and Attachments. As part of this filing, NERC requests approval as set out in **Exhibits 1, 4a, 4b, 6a, and 6b** of the filing:

- Version 3 CIP Standards and associated changes to VRFs and VSLs;
- Revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to become effective on April 1, 2010;
- Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3; and
- Carrying forward Version 2 VRFs and VSLs for un-modified requirements from Version 2.

[9] *See* also the previous discussion on decreasing reliance on technical feasibility exceptions.

Respectfully submitted,

/s/ Holly A. Hawkins

Gerry W. Cauley
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
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

Exhibits 1 – 6b

(Available on the NERC Website at
http://www.nerc.com/fileUploads/File/Filings/CIP_V3_Attachments.pdf)