NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 8, 2011

VIA ELECTRONIC FILING

Lorraine Légère, Board Secretary
New Brunswick Board of Commissioners of Public Utilities
P.O. Box 5001
15 Market Square, Suite 1400
Saint John, NB
E2L 4Y9

Re: *North American Electric Reliability Corporation*

Dear Ms. Légère:

The North American Electric Reliability Corporation ("NERC") hereby submits this Notice of Filing of the following proposed Critical Infrastructure Protection (CIP) Reliability Standards set forth as **Exhibit A** to this notice:

- CIP-002-4– Cyber Security — Critical Cyber Asset Identification (CIP-002-4)
- CIP-003-4 – Cyber Security — Security Management Controls (CIP-003-4)
- CIP-004-4 – Cyber Security — Personnel & Training (CIP-004-4)
- CIP-005-4 – Cyber Security — Electronic Security Perimeter(s) (CIP-005-4)
- CIP-006-4 – Cyber Security — Physical Security of Critical Cyber Assets (CIP-006-4)
- CIP-007-4 – Cyber Security — Systems Security Management (CIP-007-4)
- CIP-008-4 – Cyber Security — Incident Reporting and Response Planning (CIP-008-4)
- CIP-009-4 – Cyber Security — Recovery Plans for Critical Cyber Assets (CIP-009-4).

These proposed reliability standards were approved by the NERC Board of Trustees on January 24, 2011.

Additionally, NERC provides notice of the associated implementation plans for CIP-002-4 through CIP-009-4 that call for the retirement of CIP-002-3 through CIP-009-3 and a new effective date that will be determined in accordance with approval of the proposed standards and the Implementation Plan included in **Exhibit B** of this filing.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

This filing discusses the proposed CIP Reliability Standards, including justification for the proposed standards and associated implementation plans.

This filing consists of the following:

- This transmittal letter;
- A table of contents;
- A narrative description providing justification for the proposed CIP Reliability Standards;
- The proposed CIP Reliability Standards (**Exhibit A**);
- The associated Implementation Plan for the proposed CIP Reliability Standards (**Exhibit B**);
- The associated Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for the proposed CIP Reliability Standards (**Exhibit C**);
- The Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706 (**Exhibit D**);
- The Development Record of the proposed CIP Reliability Standards and the associated Implementation Plan (**Exhibit E**); and
- A table of proposed CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval (**Exhibit F**).

Please contact me if you have any questions regarding this filing.

Respectfully submitted,

/s/ Holly A. Hawkins
Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection for North American Electric Reliability Corporation

BEFORE THE
MINISTRY OF ENERGY
OF THE PROVINCE OF NEW BRUNSWICK

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF CRITICAL INFRASTRUCTURE PROTECTION (CIP) RELIABILITY STANDARDS VERSION 4

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior 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

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

June 8, 2011

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") hereby provides notice of the following proposed Reliability Standards:

- CIP-002-4 – Cyber Security — Critical Cyber Asset Identification (CIP-002-4)
- CIP-003-4 – Cyber Security — Security Management Controls (CIP-003-4)
- CIP-004-4 – Cyber Security — Personnel & Training (CIP-004-4)
- CIP-005-4 – Cyber Security — Electronic Security Perimeter(s) (CIP-005-4)
- CIP-006-4 – Cyber Security — Physical Security of Critical Cyber Assets (CIP-006-4)
- CIP-007-4 – Cyber Security — Systems Security Management (CIP-007-4)
- CIP-008-4 – Cyber Security — Incident Reporting and Response Planning (CIP-008-4)
- CIP-009-4 – Cyber Security — Recovery Plans for Critical Cyber Assets (CIP-009-4)

The NERC Board of Trustees approved the proposed Reliability Standards on January 24, 2011 and recommended they be added to the NERC Reliability Standards. In this filing, NERC provides notice of the proposed Reliability Standards and the associated implementation plans for the CIP Reliability Standards. These standards will become effective on the first day of the eighth calendar quarter after approval of CIP-002-4 through CIP-009-4.

Exhibit A to this filing sets forth the proposed Reliability Standards. **Exhibit B** contains the Implementation Plan for the CIP Reliability Standards that are being submitted. **Exhibit C** contains the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for the CIP Reliability Standards that are being submitted. **Exhibit D** contains the Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706, which was the technical team responsible for developing the proposed CIP Reliability Standards and associated Implementation Plans. **Exhibit E** contains the development record for the proposed CIP Reliability Standards and associated Implementation Plans. **Exhibit F** contains a table of CIP Version 4 Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs").

NERC filed the proposed CIP Reliability Standards and associated documents with the Federal Energy Regulatory Commission ("FERC"), and is also filing the proposed CIP

Reliability Standards and association documents with the other applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

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

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior 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

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

III. BACKGROUND

a. Basis for Proposed Reliability Standard

The proposed CIP Reliability Standards serve the important reliability goal of providing a cyber security framework for the identification and protection of Critical Cyber Assets to support the reliable operation of the Bulk Electric System.

The proposed CIP-002-4 Reliability Standard improves reliability by:

- establishing uniform criteria across all Responsible Entities for the identification of Critical Assets,
- establishing a list of Critical Cyber Assets for each Responsible Entity based on its list of Critical Asserts, and

- requiring updates to each list as necessary and an annual review.

Additionally, the proposed CIP Reliability Standards CIP-003-4, CIP-004-4, CIP-005-4, CIP-006-4, CIP-007-4, CIP-008-4, and CIP-009-4 are being submitted with conforming changes to the version numbers, the Applicability section, and the Compliance Enforcement Authority sections.

b. Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC *Standard Processes Manual*, which is incorporated into the Rules of Procedure as Appendix 3A. NERC's 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 for submission to the applicable governmental authorities.

The work culminating in this filing originated in FERC Order No. 706.[1] FERC Order No. 706 at Paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶61,040 (January 18, 2008) ("Order No. 706").

assessment; (4) external review of critical assets identification; and (5) interdependency analysis.[2]

Prior to the development of the proposed CIP Version 4 Reliability Standards, the Standard Drafting Team developed the CIP-002-2 through CIP-009-2 standards to comply with the near-term, specific directives of FERC Order No. 706. That version of the standards was approved by FERC on September 30, 2009 with additional directives to be addressed within 90 days of the order.[3] In response, the standard drafting team developed the CIP-003-3 through CIP-009-3 standard.[4]

The standard drafting team has continued efforts to address the remaining FERC Order No. 706 directives. The team limited the scope of requirements in the development of CIP-002-4 through CIP-009-4 as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236. The standard drafting team is continuing to address the remaining FERC Order No. 706 directives. The next version of the CIP-002 through CIP-009 Reliability Standards will build on the CIP-002-4 standards' establishment of uniform criteria for the identification of Critical Assets. Given this approach, no Responsible Entity's work toward compliance with the proposed Version 4 CIP Reliability Standards will be wasted. A phased approach to meeting the directives in FERC Order No. 706 has consistently built upon prior versions of the CIP-002 through CIP-009 standards to enhance the reliability of the Bulk Electric System. While the standard drafting team is still working to determine what form the next version of the CIP Reliability Standards will take, with the revisions in Version 4, an established baseline of cyber protection will be extended to all Bulk Electric SystemCritical Assets.

---

[2] *Id.* at P 236.
[3] *Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶61,291 (September 30, 2009) ("September 30, 2009 Order").
[4] *Order on Compliance,* 130 FERC ¶61, 271 (March 31, 2010) ("March 31, 2010 Order").

The proposed CIP-002-4 through CIP-009-4 Reliability Standards provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. The proposed CIP-002-4 standard requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the "bright-line" criteria contained in Attachment 1 – Critical Asset Criteria of the CIP-002-4 standard. The remaining CIP Reliability Standards, CIP-003-4 through CIP-009-4, contain conforming changes to match the versioning of CIP-002-4. There are no substantive changes to those standards.

The proposed CIP Reliability Standards set out in **Exhibit A** have been developed and approved by industry stakeholders using NERC's *Reliability Standards Development Procedure* and its replacement, the NERC *Standards Processes Manual*.[5] The proposed CIP Reliability Standards were approved by the NERC Board of Trustees on January 24, 2011.

[5] NERC's *Reliability Standards Development Procedure* is available on NERC's website at http://www.nerc.com/fileUploads/File/Standards/RSDP_V6_1_12Mar07.pdf. Note that FERC approved the new Reliability *Standard Processes Manual* on September 3, 2010 (FERC Docket No. RR10-12-000), which replaces the *Reliability Standards Development Procedure Version 7* in its entirety. NERC developed this standard in accordance with the *Reliability Standards Development Procedure Version 7* until the *Standard Processes Manual* was approved on September 3, at which time that procedure was used to complete development of the proposed standards.

IV. JUSTIFICATION FOR PROPOSED MODIFICATIONS TO RELIABILITY STANDARDS

a. Section Overview

This section summarizes the development of the proposed CIP Reliability Standards. The discussion in this section is also intended to demonstrate that the proposed modifications to the CIP Reliability Standards ensure that they are just, reasonable, not unduly discriminatory or preferential and in the public interest.

Exhibit A to this filing sets forth the proposed Reliability Standards. **Exhibit B** contains the Implementation Plan for the CIP Reliability Standards that are being submitted. **Exhibit C** contains the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for the CIP Reliability Standards that are being submitted. **Exhibit D** contains the Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706 that was responsible for drafting the proposed CIP Reliability Standards and associated Implementation Plans. **Exhibit E** contains the development record for the proposed CIP Reliability Standards and associated Implementation Plans. **Exhibit F** contains a table of CIP Version 4 VRFs and VSLs

This extensive development record includes successive drafts of the standard, the ballot pool, the final ballot results by registered ballot body members, and stakeholder comments received during the development of the proposed CIP Reliability Standards, as well as a discussion regarding how those comments were considered in developing them.

The proposed CIP-002-4 Reliability Standard requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1 of CIP-002-4.

The following changes were made to the approved Reliability Standard CIP-002-3 in the development of CIP-002-4:

- The Applicability section was modified to include an exemption for nuclear facilities regulated by the Canadian Nuclear Safety Commission, and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54;
- Requirement R1, which required Responsible Entities to identify and document a risk-based assessment methodology to identify Critical Assets was modified;
- Requirement R2 was modified to replace the risk-based assessment methodology with a set of uniform criteria for identifying Critical Assets provided in Attachment 1;
- Requirement R3 was modified to provide direction on how to identify shared Cyber Assets at generation plant sites;
- Requirement R4 was modified to remove the reference to risk-based assessment methodology;
- Measure M3 was modified to clarify what records Responsible Entities were required to retain;
- The Compliance section was modified to clarify the Compliance Enforcement Authority under various scenarios; and
- Attachment 1 was added to provide uniform criteria for the identification of Critical Assets.

The remaining CIP Reliability Standards CIP-003-4 through CIP-009-4 contain proposed changes conforming to the CIP-002-4 standard.

The Applicability section in CIP-002-3 was modified to include an exemption for nuclear facilities regulated by the Canadian Nuclear Safety Commission, and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54. The "Rationale and Implementation Reference Document" that was posted during the balloting process,[6] provides guidance for and clarification of Attachment 1 of CIP-002-4. Attachment 1 describes the Critical Asset Criteria a covered entity shall consider in identifying its Critical Assets. This document states on page 6 that "these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies since they are regulated outside of NERC jurisdiction." Additionally, this document provides that "[t]here may be facilities, equipment, or systems which may be in a nuclear facility associated with the Bulk Electric System which are outside of the regulatory realm of these nuclear organizations." This guidance, in conjunction with the exemption included in Section 4.2.3 of the proposed CIP-002-4 standard, provides that a U.S. nuclear power plant facility that has a verified cyber security plan under 10 C.F.R. Section 73.54 which includes all nuclear power plant systems, structures, and components is exempt from CIP-002-4 requirements, and therefore is not responsible for complying with the CIP-002-4 requirements, including the Critical Asset Identification requirement in Requirement R1 and Attachment 1. If any nuclear power plant systems, structures, and components are not covered under a verified cyber security plan, those systems, structures, and components must be evaluated for CIP-002-4 applicability.

All prior approved versions of CIP-002 included as the first requirement (Requirement R1): "Critical Asset Identification Method — The Responsible Entity shall identify and

[6] *See,* http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean_20101220.pdf,

document a risk-based assessment methodology to use to identify its Critical Assets." This Requirement R1 lists certain assets that must be considered when identifying Critical Assets.

In FERC Order No. 706 at Paragraph 253, FERC stated that: "the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets." FERC therefore directed NERC, in its discretion, to: "incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. " In addition, FERC provided in Order No. 706 that: "… we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System."

In response to these directives, NERC developed guidance documents intended to be used to assist entities in developing their risk-based methodology and Critical Asset identification. Over the past two years NERC has conducted various reviews of risk-based methodologies developed by many entities of varying sizes to comply with CIP-002 Requirement R1 and determined that the existing methodologies generally do not adequately identify all Critical Assets. Accordingly, NERC charged the standard drafting team with developing bright line criteria that could be used to identify Critical Assets rather than relying on an entities' existing risk-based methodology. These criteria are provided in Attachment 1 of the proposed CIP-002-4 standard. With these bright line criteria, NERC fulfills the two Order No. 706 directives identified above.

Because Responsible Entities will no longer have a requirement to develop a risk-based assessment methodology, Requirement R2 of the existing CIP-002-3 standard was modified to replace the risk-based assessment methodology for Critical Asset identification with the criteria

provided in Attachment 1of CIP-002-4. This requirement now becomes Requirement R1 of the proposed CIP-002-4 standard.

Requirement R3 of the existing CIP-002-3 standard was modified to provide direction on how to identify shared Cyber Assets at generation plant sites. This requirement now becomes Requirement R2 of CIP-002-4.

Criterion 1.1 of Attachment 1exists to ensure that generation Facilities with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Requirement R2 of the proposed CIP-002-4 standard further stipulates that, for Generation Facilities, only those Cyber Assets that are shared by any combination in a group of units that would exceed this value are candidates for further qualification as Critical Cyber Assets (*i.e.*, the Critical Asset is the group of units that exceeds the specified value). In considering common mode vulnerabilities, the Responsible Entity should include all Facilities and systems up to the point where the Generation is attached to the transmission system. In specifying a 15-minute qualification, Requirement R2 includes only those Cyber Assets that would have a real-time impact on the reliable operation of the Bulk Electric System.

In a generation facility context, there may be Facilities which, while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes. This is illustrated in the case of cyber assets controlling the supply of coal fuel in a coal burning facility. In this case, the compromise of the cyber asset may result in an inability of the supply system to bring the fuel for generation. However, because of the way these systems are used, there may be a significant amount of time before this affects real-time operation—time during which detection and remediation may be able to be effected.

Requirement R2 and Criterion 1.1 of Attachment 1 both reference a "group of generating units (including nuclear generation) at a single plant location. . . ." This language refers only to generation owners or operators with multiple generators at a single plant location (***e.g.,*** gas and nuclear generation at a single site). In the case of nuclear generation, the only Cyber Assets that would be evaluated are those that are not covered under a verified cyber security plan under 10 C.F.R. Section 73.54.

Requirement R4 of CIP-002-3 was modified to remove the reference to risk-based assessment methodology. This requirement now becomes Requirement R3 of CIP-002-4.

Attachment 1 of CIP-002-4 provides uniform criteria for the identification of Critical Assets across all Responsible Entities. A form of these criteria was first proposed in a version of CIP-002-4 that was posted for informal industry comment on December 19, 2009. The standard drafting team analyzed comments from industry and subsequently posted a new document for industry comment—CIP-010-1—on May 4, 2010. The team analyzed these comments from industry and continued to refine the criteria.

NERC then issued a data request to the industry, in accordance with Section 1600 of the NERC Rules of Procedure, in order to gather empirical data that could be used to guide the determination of the final criteria used in the development of the CIP-002-4 standard. Section 1600 of the NERC Rules of Procedure gives NERC the authority to request data or information that is deemed necessary to meet its obligations. The results of this data request were analyzed and used to develop a new proposed CIP-002-4 standard that was posted for industry comment on October 20, 2010. After two ballot and comment periods, the industry approved the CIP-002-4 standard and the associated Attachment 1.

The following discussion is an analysis of each of the criterion included in Attachment 1, including the applicable responses from the NERC data request. Each criterion is listed, followed by a summary of the NERC data request responses. Each section concludes with a discussion of the justification for each criterion.

Criterion 1.1

1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

NERC Data Request (summary results in parenthesis):

1.1. Nuclear generation Facilities. (17 using CIP-002-3, 88 using this criterion)

1.2. A generating unit or a group of generating units at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding: (59 using CIP-002-3, 229 using this criterion)

a. the Contingency Reserve requirement of the Reserve Sharing Group or of the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the CIP-002 is reviewed, or

b. the lowest value of the Contingency Reserve requirement of the associated Balancing Authority, for the 12 months preceding the identification or reassessment of the group of generating units, or

c. 2000 MW.

The drafting team, after much debate and evaluation of comments, determined that a Bulk Electric System reliability criterion should not be solely based on fuel type. In addition, the team received feedback that the wording of item 1.2 in the data request was confusing, that the

amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team therefore performed an informal survey of the Regional Entities and identified what the megawatt value of the reserve sharing would be for various groups. The Regional Entities sourced this criterion partly from the Contingency Reserve requirements in the NERC BAL-002 Reliability Standard, the purpose of which is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, BAL-002 requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." Additionally, regarding the use of net Real Power capability, the standard drafting team sought to use a value that could be verified through the existing MOD-024 requirements.

The standard drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Balancing Authorities in all regions. Using this number and data reported by the U.S Energy Information Administration at http://www.eia.doe.gov/cneaf/electricity/page/capacity/existingunits2008.xls, the team determined that approximately 146 generators in the United States would be classified as Critical Assets using this criterion. This accounts for 29% of the installed generator capacity in the United States.

Criterion 1.2

1.2 Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

NERC Data Request (summary results in parenthesis):

1.3. Any reactive resource, including synchronous condensers and static VAR compensators not associated with Generation Facilities, sharing a common Cyber Asset or common Cyber Assets, excluding control centers, that would have an impact on the reliable operation of the group of Facilities within 15 minutes, singularly or in combination, with aggregate rated net Reactive Power capability of 1,000 MVAR or more. (9 using CIP-002-3, 22 using this criterion)

The team received comments that some of the questions in the Data Request were difficult to understand. One of the main reasons this particular criterion caused confusion was that it defined Critical Assets by using Critical Cyber Assets, which are not evaluated until Requirement R3. After careful consideration, the team determined that Criterion 1.2 in CIP-002-4 captured the same facilities that were captured in Item 1.3 of the NERC Data Request. However, the nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. Therefore, the value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

Criterion 1.3

1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

NERC Data Request (summary results in parenthesis):

1.4 Any generation Facility that the Planning Coordinator identifies as Reliability "must run" assigned units. (14 using CIP-002-3, 44 using this criterion)

The drafting team sought to ensure that those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid Bulk Electric System Adverse

Reliability Impacts in the long term planning horizon are designated as Critical Assets. These Facilities may be designated as "Reliability Must Run," which is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement using terms included in the NERC Glossary. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation. The standard drafting team does not believe that the changes from the NERC Data Request to criterion 1.3 will result in a significant change to the number of assets indentified as a Critical Asset.

Regarding the "long-term planning horizon" criterion, the standard drafting team sought to ensure that such Critical Assets would be designated in the time horizon described in the NERC document "Time Horizons",[7] which defines "long-term planning horizon" as "a planning horizon of one year or longer."

Criterion 1.4

1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan.

NERC Data Request (summary results in parenthesis):

1.5 Any Blackstart Resource contained in the Transmission Operator's restoration plan. (337 using CIP-002-3, 540 using this criterion)

[7] *See*, http://www.nerc.com/files/Time_Horizons.pdf.

The standard drafting team determined that the change from the NERC Data Request to criterion 1.3 would result in a significant change in the number of assets indentified as a Critical Asset. The EOP-005-2 Reliability Standard requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. Criterion 1.2 designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term "Blackstart Capability Plan" has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

In response to concerns received regarding the communication to Bulk Electric System asset owners and operators of their roles in the Restoration Plans, Transmission Operators are required, pursuant to NERC standard EOP-005-2, to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

Criterion 1.5

1.5 The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

NERC Data Request (summary results in parenthesis):

1.9. The Facilities comprising Cranking Paths contained in a Transmission Operator's restoration plan. (981 using CIP-002-3, 1598 using this criterion)

The drafting team received many questions concerning what was intended to be captured in the data request. Commenters pointed out that many options exist for Cranking Paths, and many Transmission Operators develop extensive restoration plans that include multiple Cranking Paths in order to provide flexibility to System Operators in actual restoration scenarios. This may lead to most, if not all, of their Bulk Electric System assets being declared Critical Assets, which could therefore lead to the undesirable result of eliminating those options in restoration plans going forward. Based on these comments, the standard drafting team determined that the most critical elements in the Cranking Path are the points at which no options exist for the System Operator. While it cannot be determined with certainty how the change will affect the final Critical Asset numbers, the standard drafting team believes that at a minimum, currently declared Critical Assets using existing risk based methodologies will remain on future Critical Asset lists. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

Criterion 1.6

1.6 Transmission Facilities operated at 500 kV or higher.

NERC Data Request (summary results in parenthesis):

1.6. Transmission Facilities operated at 500kV or higher. (270 using CIP-002-3, 436 using this criterion)

There was no change from what was included in the Data Request to criterion 1.6. Therefore there is no expected change to the numbers reported. While the standard drafting team believes that Facilities operated at 500 kV or higher did not require any further qualification for their role as Critical Assets to the interconnected Bulk Electric System, Facilities in the lower

Extra High Voltage ("EHV") range should have additional qualifying criteria for inclusion as a Critical Asset.

It should be noted that if the collector bus for a non-Critical Asset generation plant (*i.e.*, the plant is smaller in aggregate than the threshold set for generation plants in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." Therefore, this collector bus would not be a Critical Asset because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the Critical Asset threshold.

Criterion 1.7

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

NERC Data Request (summary results in parenthesis):

1.7. Transmission Facilities with four or more Transmission lines operated at 300 kV or higher in the Eastern Interconnection or the Western Interconnection. (140 using CIP-002-3, 224 using this criterion)

1.8. Transmission Facilities with four or more Transmission lines operated at 200 kV or higher in the Texas Interconnection or the Quebec Interconnection. (48 using CIP-002-3, 115 using this criterion)

The threshold for the criterion was lowered from four to three in the Eastern and Western Interconnection, and raised from 200 kV to 300kV in the Texas Interconnection and the Quebec Interconnection. Based on the survey results, the standard drafting team believes that more

Facilities will be captured under criterion 1.7 than the criterion included in the Data Request. Criterion 1.7 includes the lower end of the EHV range for Transmission Facilities between 300kV and 500 kV, (primarily Facilities operated at 345kV) with qualifications for inclusion as Critical Assets if they are deemed highly likely to have a significant impact on the Bulk Electric System. While the criterion has been specified as part of the rationale for requiring protection for EHV Transmission Facilities, the standard drafting team also included additional qualifications that would ensure the required level of impact to the Bulk Electric System. At the lower end of the EHV spectrum, the drafting team excluded radial facilities that would only provide support for single generation facilities and specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

Criterion 1.8

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

NERC Data Request (summary results in parenthesis):

1.10 Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). (115 using CIP-002-3, 151 using this criterion)

Commenters stated that Item 1.10 in the data request was confusing for entities to determine the applicability if this item, because a change in operation of a Transmission Facility does not violate an IROL. The standard drafting team revisited the intent behind the criterion, which was to include those Transmission Facilities that have been identified as critical to the

derivation of IROLs and their associated contingencies, as specified by FAC-014-2—Establish and Communicate System Operating Limits, Requirements R5.1.1 and R5.1.3. The criterion was changed to reflect this, and the standard drafting team now believes that more Facilities will be captured with the revised criterion than the criterion included in the Data Response.

Criterion 1.9

1.9 Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

NERC Data Request (summary results in parenthesis):

1.11. Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs). (0 using CIP-002-3, 0 using this criterion)

Commenters noted that Item 1.11 in the data request was confusing for entities to determine the applicability of this Item because a change in operation of a Transmission Facility does not violate an IROL. The team revisited the intent behind the criterion and FAC-014.2, which is to include those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2—Establish and Communicate System Operating Limits, Requirements R5.1.1 and R5.1.3. The wording of criterion 1.9 was changed to reflect this intent. The standard drafting team believes that as the impacts of FACTS devices become more prevalent on the Bulk Electric System, more Facilities will be captured with the revised criterion than the Data Request.

Criterion 1.10

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

NERC Data Request (summary results in parenthesis):

1.12. Transmission Facilities providing the generation interconnection that if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified in Attachment 1, criterion 1.1. (39 using CIP-002-3, 82 using this criterion)

Criterion 1.10 designates those Transmission Facilities as Critical Assets that provide the generation interconnection for generation Facilities identified as Critical Assets to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. The criterion was changed to add Transmission Facilities providing the generation interconnection for Blackstart Resources. Although the majority of these facilities will likely be captured in criterion 1.5 (Cranking Path), this criterion was added to ensure that all Transmission Facilities providing the generation interconnection for generation Critical Assets be designated as Critical Assets.

Criterion 1.11

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

NERC Data Request (summary results in parenthesis):

1.13. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for Nuclear facilities (46 using CIP-002-3, 123 using this criterion)

There were no significant changes from the data request to Criterion 1.11, therefore there is no expected impact to the numbers reported in response to the data request. Criterion 1.11 is based on NUC-001-2 R9.2.2—Identification of facilities, components, and configuration restrictions that are essential for meeting the [Nuclear Plant Interface Requirements] NPIRs." NUC-001-2 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, Requirement R9.3.6 requires "Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan."

Criterion 1.12

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

NERC Data Request (summary results in parenthesis):

1.14. Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements and that have impact beyond the local area. (105 using CIP-002-3, 158 using this criterion)

Commenters expressed concern that the phrase "impact beyond the local area" might be interpreted many different ways. After careful consideration, the standard drafting team chose to designate as Critical Assets those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure Bulk Electric System operation within IROLs. The degradation, compromise or unavailability of these Critical Assets would result in exceeding IROLs if they fail to operate as designed because IROL is defined as "A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading Outages that adversely impact the reliability of the Bulk Electric System." By using the definition of IROL, the loss or compromise of any of these Critical Assets would have Wide Area impacts, meeting the original intent of the NERC Data Request. While it cannot be determined with certainty how the change will affect the final numbers, the standard drafting team believes that, at a minimum, currently declared Critical Assets using existing risk based methodology will remain on future Critical Asset lists.

Criterion 1.13

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

NERC Data Request (summary results in parenthesis):

1.15. Common control system(s) critical to automatic load shedding that are capable of shedding 300 MW or more. (12 using CIP-002-3, 13 using this criterion)

This criterion was intended to include as Critical Assets regional Under Frequency Load Shedding ("UFLS") and Under Voltage Load Shedding ("UVLS") schemes. Some commenters

noted that including this criteria might inadvertently require all SCADA systems with the capability of shedding load to be declared as Critical Assets, even if such SCADA systems are in fact not planned or operated to perform load shedding. This was not the intent of this criterion. Other commenters stated that this item needed to be clarified to confirm that it applies to a single common control system only, and not multiple but separate "like" systems that in aggregate are capable of load shedding up to 300 MW. Additionally, the criterion needed to be clarified to confirm that it applies to systems "configured" for automatic load shedding, not simply just systems that are "capable" of load shedding.

In light of the comments received, the drafting team chose to change the criterion to specifically include only those systems that did not require human operator initiation, and targeted in particular those UFLS facilities and systems and UVLS facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of load shedding 300 MW or more. While these qualifying systems require a human operator to arm the system, once armed, they trigger automatically. Therefore the criteria to designate these systems as Critical Assets removed the human operator initiation requirement from criterion 1.13. Additionally, the 300MW threshold is consistent with prior versions of CIP-002. The standard drafting team does not believe that the change will reduce the number of systems classified as Critical Assets below the number reported in response to the NERC Data Request.

Criterion 1.14

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

NERC Data Request (summary results in parenthesis):

1.16. Any primary control center or any backup control center used to perform Reliability Coordinator functions. (44 using CIP-002-3, 38 using this criterion)

There were no changes to the criteria from the NERC Data Request to Criterion 1.14, therefore there is no expected impact to the numbers reported. A follow up to a few respondents served to clarify why the number went down. There was confusion about how to classify a control center that performs multiple functions. After further discussion with the entities, it was clear that the net number for all control centers would be a more accurate count of Critical Assets. The standard drafting team believes that the sum of Critical Assets declared under the new criteria 1.14, 1.15, 1.16, and 1.17 will total more than the sum of the responses from the NERC Data Request items 1.16, 1.17, 1.18, 1.19.

Criterion 1.15

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

NERC Data Request (summary results in parenthesis):

1.16. Any control center or systems or any backup control center or systems used to perform Generator Operator functions for generation that has an aggregate highest rated net Real Power capability in the preceding 12 months exceeding:

a. the lowest value of the Contingency Reserve requirement of the associated Balancing Authority, for the 12 months preceding the identification or reassessment of the generating unit, or

b. 2000 MW, if no Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group is established. (81 using CIP-002-3, 121 using this criterion)

The analysis used to develop criterion 1.15 is similar to the development of criterion 1.1. In addition, the drafting team believed that any generation control center that controls generation that is designated a Critical Asset must also be classified as a Critical Asset. For this reason, criteria 1.3 and 1.4 were added to the proposed CIP-002-4 standard. The standard drafting team believes that adding the additional criteria and lowering the MW threshold to 1500 MW will increase the number of systems classified as Critical Assets above the number reported in the NERC Data Survey.

Criterion 1.16

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

NERC Data Request (summary results in parenthesis):

1.18. Any primary or backup control center performing Transmission Operator functions performed by primary or backup control centers that remotely control two or more Transmission substations or switching stations operated at 300 kV or above in the Eastern Interconnection or the Western Interconnection or 200kV or above in the Texas Interconnection or the Quebec Interconnection, or functionality that remotely controls a Critical Cyber Asset with a High Impact Rating. (195 using CIP-002-3, 221 using this criterion)

Criterion 1.16 specifies that all control centers or backup control centers that perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12 is to be designated as a Critical Asset due to their direct impact on the operation of identified Critical Assets. In many cases, some Transmission Operator functions are delegated to Transmission Owner control centers. In such cases, these must also be designated as Critical Assets. The drafting team intended for the word "control" to have the same meaning as that found in "Frequently Asked Questions Cyber Security Standards CIP-002-1 through CIP-009-1" document,[8] which indicates that controls may be "performed automatically, remotely, manually, or by voice instruction." The standard drafting team believes that most, if not all, of the control centers reported in the NERC Data Survey will still qualify under the approved criterion.

Criterion 1.17

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

NERC Data Request (summary results in parenthesis):

1.17. Any primary or backup control center performing Balancing Authority functions performed by primary or backup control centers, of Transmission Facilities or generation Facilities, singularly or in combination, of 4,000 MW or more in the Eastern Interconnection or the Western Interconnections or 2,000 MW or more in

[8] *See,* http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf.

the Texas Interconnection or the Quebec Interconnection. (105 using CIP-002-3, 113 using this criterion)

The analysis used to develop criterion 1.17 is similar to the development of criterion 1.1. In addition, the standard drafting team believes that any generation Balancing Authority control center that controls generation that is designated a Critical Asset must also be classified as a Critical Asset. For this reason, criteria 1.3, 1.4, and 1.13 were added to Criterion 1.17. The standard drafting team believes that adding the additional criteria and lowering the MW threshold to 1500 MW will increase the number of systems classified as Critical Assets above the number reported in response to the NERC Data Request.

The following Item was included in the NERC Data Request but was not included as a criterion in CIP-002-4:

1.20. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include.

This item was included in the NERC Data Request to determine whether and what additional items on existing Critical Asset lists may not meet the new criteria included in Attachment 1. There were several entities that were contacted that had a significant number of entries in this category. The overwhelming response received was that these assets were placed on the Critical Asset list for reasons other than Bulk Electric System reliability. For example, some entities placed large industrial loads or other retail loads that have little impact to Bulk Electric System reliability. Others included every generator they owned, regardless of size, in their Critical Asset methodologies. In no case did the standard drafting team determine that the assets that were included in the responses to this Data Request question could also be assets that impacted Bulk Electric System reliability.

In summary, NERC believes that the application of the uniform criteria included in the proposed Attachment 1 to the CIP-002-4 Reliability Standard will result in more Bulk Electric System assets being declared as Critical Assets, as demonstrated in the analysis of each criterion included Attachment 1. This, in turn, will result in the inclusion of more Bulk Electric System assets as Critical Cyber Assets. While some entities may have a few assets taken off of its existing Critical Asset list under the criteria proposed in CIP-002-4, it is expected that, overall, more Bulk Electric System assets in North America will be classified as Critical Assets. Additionally, it is anticipated that the application of the uniform criteria in Attachment 1 will result in a more consistent identification of Critical Assets by all Responsible Entities.

The proposed CIP-002-4 Reliability Standard contains three requirements summarized as follows:

Requirement R1 mandates that each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

Requirement R2 mandates that each Responsible Entity shall develop a list of Critical Cyber Assets associated with the list of Critical Assets developed in Requirement R1. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of the CIP-002-4 standard, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

Requirement R3 mandates that a senior manager or delegate for each Responsible Entity shall approve annually the list of Critical Assets and the list of Critical Cyber Assets, even if that list contains no elements.

b. Demonstration that the proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential and in the public interest

1. Proposed Reliability Standards are designed to achieve a specified reliability goal

The proposed CIP Reliability Standards provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets. Proposed Reliability Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.

2. Proposed Reliability Standards contains a technically sound method to achieve the goal

The proposed CIP Reliability Standards achieve their stated goal of providing a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. Specifically, the proposed Reliability Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria included in Attachment 1 of the proposed CIP-002-4 standard.

Requirement R1 mandates that each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. This will ensure that each Responsible Entity evaluates its entire portfolio of Bulk Electric System assets against the criteria in Attachment 1 to determine those assets that are critical to the reliable operation of the Bulk Electric System.

Requirement R2 mandates that each Responsible Entity shall develop a list of Critical Cyber Assets associated with its list of Critical Assets developed in response to Requirement R1. This will ensure that each Responsible Entity examines each Critical Asset to find any Cyber Asset that could impact the real time operation of the Critical Asset.

Requirement R3 mandates that a senior manager or delegate for each Responsible Entity shall approve annually the list of Critical Assets and the list of Critical Cyber Assets, even if that list contains no elements. This will ensure that the senior management for each Responsible Entity has verified that Requirements R1 and R2 have been properly performed and validated.

The rest of the CIP Reliability Standards mandate the minimum protection that must be provided to Critical Cyber Assets. Reliability Standard CIP-003-4 requires that Responsible

Entities have minimum security management controls in place to protect Critical Cyber Assets. Reliability Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Reliability Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Reliability Standard CIP-006-4 ensures the implementation of a physical security program for the protection of Critical Cyber Assets. Reliability Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Reliability Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Reliability Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

The proposed CIP Reliability Standards have been developed by a standard drafting team with a broad base of Bulk Electric System and cyber security knowledge following the scope identified in the Standard Authorization Request that resulted in the initiation of NERC Project 2008-06 Cyber Security Order 706. The standard drafting team for this project adhered to NERC's standards development process, which allows for industry comment and ballot of the proposed standards. Extensive industry comments on the proposed standards were received and evaluated through several postings. Many of the comments have been incorporated into the final draft of the standards, resulting in refined, high quality standards.

3. Proposed Reliability Standards are applicable to users, owners, and operators of the bulk power system, and not others

The proposed CIP Reliability Standards are applicable only to Reliability Coordinators, Balancing Authorities, Interchange Authorities, Transmission Service Providers, Transmission Owners, Transmission Operators, Generator Owners, Generator Operators, Load Serving Entities, NERC, and Regional Entities. These entities are users, owners, or operators of the bulk power system,

4. Proposed Reliability Standards are clear and unambiguous as to what is required and who is required to comply

Each of the requirements in the proposed CIP-002-4 Reliability Standard is clear in identifying the required performance (what) and the responsible entity (who):

> Requirement R1 - Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.
>
> Requirement R2 - Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.
>
> For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

Requirement R3 - Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 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.)

The remaining proposed CIP Reliability Standards, CIP-003-4 to CIP-009-4, retain the same requirement language as the previous standards and have already been determined to meet this criterion.

5. Proposed Reliability Standards include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation

Each primary requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in Reliability Standards, as defined in the ERO Sanction Guidelines. The table included in **Exhibit F** shows the VRFs and VSLs resulting in the indicated range of penalties for violations.

6. Proposed Reliability Standards identify clear and objective criterion or measures for compliance, so that it can be enforced in a consistent and non-preferential manner

The proposed CIP Reliability Standards identify clear and objective criteria in the language of the requirements so that that the standards can be enforced in a consistent and non-preferential manner. The language in the requirements is unambiguous with respect to the applicable entity expectations. Each requirement has a single associated measure.

7. Proposed Reliability Standards achieve a reliability goal effectively and efficiently, but do not necessarily have to reflect "best practices" without regard to implementation cost

The proposed CIP Reliability Standards helps the industry achieve the stated goals of identifying Critical Assets and Critical Cyber Assets to ensure Bulk Electric System reliability effectively and efficiently. While there may be an increase in implementation costs as the number of Critical Assets increase under the methodology in proposed CIP-002-4, the NERC Board of Trustees and the industry approved the revised methodology because there is recognition that it is needed to help ensure bulk power system reliability. Accordingly, the costs associated with implementing the proposed CIP-002-4 through CIP-009-4 Reliability Standards are not determined to be excessive or unreasonably burdensome.

8. Proposed Reliability Standards are not "lowest common denominator," i.e., do not reflect a compromise that does not adequately protect bulk power system reliability

The proposed CIP Reliability Standards do not aim at "lowest common denominator." The proposed CIP-002-4 standard provides clear and uniform criteria for identifying Critical Assets on the Bulk Electric System. The remaining proposed CIP Reliability Standards, CIP-003-4 to CIP-009-4, retain the same requirement language as the previous standards and have already been determined to meet this criterion.

9. ***Proposed Reliability Standards consider costs to implement for smaller entities but not at consequence of less than excellence in operating system reliability***

The proposed CIP Reliability Standards do not create any differentiation in requirements based on size. All entities, small and large, are expected to comply with these standards in the same manner.

10. Proposed Reliability Standards are designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one area or approach

The requirements in the proposed CIP Reliability Standards apply throughout North America, with no exceptions. The proposed CIP Reliability Standards are a set of standards that will be universally applicable in the portions of the United States and Canada that recognize NERC as the ERO.

11. Proposed Reliability Standards cause no undue negative effect on competition or restriction of the grid

The proposed CIP Reliability Standards enhance the operation and reliability of the grid and do not constrain competition or restrict transmission capability. The purpose of the proposed CIP Reliability Standards is to provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

Specifically, Reliability Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. Proposed CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate

level of personnel risk assessment, training, and security awareness. CIP-005-4 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. CIP-006-4 ensures the implementation of a physical security program for the protection of Critical Cyber Assets. CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

The proposed CIP Reliability Standards do not have a business practice impact and thus will not result in a negative effect on competition.

12. The implementation time for the proposed Reliability Standards is reasonable

The Implementation Plan (attached as **Exhibit B**) and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (attached as **Exhibit C**) are reasonable. The Implementation Plan provided in **Exhibit B** specifies how Responsible Entities should transition during the timeframe from acceptance of the proposed CIP Version 4 standards until the Effective Date of the proposed standards. The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities included in **Exhibit C** specifies how Responsible Entities should handle newly identified Critical Cyber Assets and newly Registered Entities following the Effective Date of the proposed CIP Reliability Standards.

Based on precedent and lessons learned from past practice, NERC believes the length of time between approval of the proposed CIP Version 4 standards and the effective date is reasonable. This implementation plan time period is consistent with the implementation plan for Version 1 of the CIP Reliability Standards and the implementation plan approved for Registered Entities identifying their first Critical Cyber Asset. Additionally, it takes time to perform a thorough examination of all Bulk Electric System assets to determine whether they meet the criteria included in Attachment 1. Furthermore, additional time must be spent evaluating each Critical Asset to determine all Critical Cyber Assets. In addition, new equipment may have to be installed by Responsible Entities in order to meet the requirements of the CIP-003-4 through CIP-009-4 Reliability Standards.

The following scenarios are provided to further clarify potential implementation issues:

Scenario 1: A newly registered entity that is subject to the CIP Reliability Standards or an existing Responsible Entity identifies a new Critical Cyber Asset prior to acceptance of these proposed CIP Reliability Standards. Under this scenario the entity is subject to the requirements in CIP-002-4 to CIP-009-4 and shall use the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for Version 3.[9]

Scenario 2: Upon acceptance of these proposed CIP Reliability Standards, a Responsible Entity has existing Critical Cyber Assets and has additional assets that now meet the uniform criteria in Attachment 1 of CIP-002-4 that were not previously identified using its established risk-based identification methodology. Under this scenario the Responsible Entity shall use the Implementation Plan in Exhibit B, which specifies that Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard or (ii) the compliance milestones specified in Version 3 of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. Since these Critical Cyber Assets were not identified using CIP-002-3, the Version 3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities does not apply. Hence, the Responsible Entity shall be compliant with CIP-002-4 through CIP-009-4 for those previously existing Critical Cyber Assets as well as those additional assets captured by the

[9] *See*, http://www.nerc.com/docs/standards/sar/Imp-Plan_Newly_Identified_CCA_RE_clean_last_approval_2009Nov19.pdf.

uniform criteria in Attachment 1 of CIP-004 on the Effective Date of these propose CIP Reliability Standards.

Scenario 3: Upon acceptance of these proposed CIP Reliability Standards, a Responsible Entity has no existing Critical Cyber Assets and has assets that now meet the uniform criteria in Attachment 1 of CIP-002-4 that were not previously identified using its established risk-based identification methodology. Under this scenario, similar to Scenario 2, the Responsible Entity shall use the Implementation Plan in Exhibit B, which specifies that Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of: (i) the Effective Date specified in the Standard, or (ii) the compliance milestones specified in Version 3 of the Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities. Again, since these assets were only identified using CIP-002-4 and not CIP-002-3, the Version 3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is not applicable, so the Responsible Entity shall be compliant on the Effective Date of these proposed CIP Reliability Standards.

Scenario 4: After the Effective Date of these proposed CIP Reliability Standards, an entity is newly registered as a Registered Entity that is subject to the CIP Reliability Standards or an existing Responsible Entity identifies a new Critical Cyber Asset. Under this scenario the entity is subject to the requirements in CIP-002-4 to CIP-009-4 and shall use the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for Version 4.

Scenario 5: A Responsible Entity that has existing Critical Cyber Assets installs a new Critical Cyber Asset. All new installations of Critical Cyber Assets are required to be compliant upon commissioning, whether under CIP-002-3 to CIP-009-3 or CIP-002-4 to CIP-009-4.

Scenario 6: A Responsible Entity commissions a new planned Bulk Electric System asset 1 month prior to the Effective Date of Version 4. This asset was not determined to be a Critical Asset according to the Entity's Version 3 established risk-based identification methodology, but does meet the uniform criteria in Attachment 1 of CIP-002-4. Under this scenario, the Responsible Entity should be able to determine that the asset will meet the uniform criteria during its planning phase and therefore must be compliant with CIP-002-4 through CIP-009-4 on the Effective Date of these proposed CIP Reliability Standards.

Scenario 7: Prior to the Effective Date of these proposed CIP Reliability Standards, a Responsible Entity that previously had no existing Critical Cyber Assets identifies a new Critical Cyber Asset based upon its existing CIP-002-3 processes and procedures. In addition, this Critical Cyber Asset is associated

> with a Critical Asset that also meets the uniform criteria in Attachment 1 of CIP-002-4. Under this scenario, the Responsible Entity shall initially determine its Version 3 compliance milestones using the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for Version 3. However, the Responsible Entity may find, if the Critical Cyber Asset was identified after acceptance of these proposed CIP Reliability Standards, that its Version 3 compliance milestones are later than the Effective Date of Version 4, at which point the Version 3 CIP Reliability Standards are already retired. In such a scenario, the Responsible Entity shall use part (ii) of the Implementation Plan in Exhibit B, which specifies that Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on...the compliance milestones specified in Version 3 of the Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities. This phrase in the Version 4 Implementation Plan was included specifically to ensure that the Effective Date of these proposed CIP Reliability Standards does not override a Responsible Entity's previously established compliance milestone schedule.

13. The Reliability Standard development process was open and fair

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure, the NERC *Reliability Standards Development Procedure,* and its replacement NERC *Standards Processes Manual*, which is incorporated into the Rules of Procedure as Appendix 3A. NERC's 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 for submission to the applicable governmental authorities. The drafting team developed this standard by following NERC's regulatory-approved standards development process.

14. Proposed Reliability Standards balance with other vital public interests

The proposed CIP Reliability Standards do not conflict with any vital public interests. Compliance with these proposed CIP Reliability Standards support preventing instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the interconnection.

15. Proposed Reliability Standards consider any other relevant factors

No other factors were identified in the development of the proposed CIP Reliability Standards.

c. Violation Risk Factor and Violation Severity Level Assignments

NERC is proposing VRFs and VSLs for CIP Version 4 in this filing consistent with those proposed for CIP Version 3. On January 21, 2010, NERC submitted a Notice of Filing of CIP Version 2 VRFs and VSLs, which were carried over, in part, from the FERC-approved CIP Version 1 VRFs and VSLs and a Notice of Filing of CIP Version 3 VRFs and VSLs, which were carried over, in part, from the CIP Version 2 VRFs and VSLs.FERC issued an Order on January 20, 2011 approving the CIP Version 2 and Version 3 VRFs and VSLs, and directed that a compliance filing be made within 60 days (by March 21, 2011) that modifies certain of the CIP Version 2 and Version 3 VRFs and VSLs in response to FERC's concerns.[10]

In this filing, NERC is proposing to carry over the CIP Version 4 VRFs and VSLs from CIP Version 3. However, given that the CIP Version 4 standards were developed with proposed VSLs and VRFs prior to FERC's issuance of the January 20, 2011 Order, NERC recognizes that the proposed CIP Version 4 VRFs and VSLs included in **Appendix F** of this filing do not

[10] *Order on Version 2 and Version 3 Violation Risk Factors and Violation Severity Levels for Critical Infrastructure Protection Reliability Standards,* 134 FERC ¶61,045 (January 20, 2011).

respond to FERC's concerns articulated in the January 20, 2011 Order. Accordingly, NERC is hereby submitting with this filing the proposed CIP Version 4 VRFs and VSLs that were balloted with the proposed CIP Version 4 standards prior to the issuance of the January 20, 2011 Order. NERC will make a compliance filing in response to the January 20, 2011 Order proposing modifications to the CIP Version 2 and Version 3 VRFs and VSLs by March 21, 2011. In that filing, NERC will include an updated table of proposed VRFs and VSLs for CIP Version 4, carried over from those proposed for CIP Versions 2 and 3 VRFs and VSLs in compliance with FERC directives, and will request that those VRFs and VSLs be applied to the pending CIP Version 4 standards, as applicable.

V. SUMMARY OF THE RELIABILITY STANDARD DEVELOPMENT PROCEEDINGS

a. Development History

FERC Order No. 706 at Paragraph 236 directed NERC to develop modifications to the CIP-002-1 Cyber Security – Critical Cyber Asset Identification Reliability Standard to address concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.

A standards drafting team was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The standard drafting team has been charged with reviewing each of the CIP Reliability Standards to address the modifications identified in FERC Order No. 706. The standard drafting team began meeting in October 2008.

Prior to this filing, the standard drafting team developed the CIP-002-2 through CIP-009-2 Reliability Standards to comply with the near-term specific directives of FERC Order No. 706. The CIP Version 2 standards were approved by FERC in the September 30, 2009 Order with additional directives to be addressed within 90 days of the order. In response, the standard drafting team developed the CIP-003-3 through CIP-009-3 Reliability Standards, which were approved by FERC in the March 31, 2010 Order.

Throughout this period, the standard drafting team has continued its efforts to develop an approach to address the remaining FERC Order No. 706 directives. Most recently, the proposed CIP-010 and CIP-011standards were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the standard drafting team determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the standard drafting team limited the scope of requirements in this Version 4 of CIP-002 through CIP-009 as an interim step to address the more immediate concerns raised in Paragraph 236 of Order No. 706. The plan to address the remaining FERC Order No. 706 directives continues to be developed.

On September 20, 2010, the standard drafting team posted the proposed CIP-002-4 standard for a formal 45-day comment period. During the comment period, the team received 101 sets of comments, including comments from more than 200 different people from approximately 125 companies representing 9 of the 10 Industry Segments. Concurrent with the comment period, a ballot pool was assembled and the first formal ballot was conducted. In the initial ballot, a quorum was achieved, and the weighted sector vote was 43.33% affirmative.

Based on the comments received, a few changes were made to the CIP-002-4 standard. The Applicability section was modified to include an exemption for nuclear facilities regulated

by the Canadian Nuclear Safety Commission and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54. In addition, the effective date was changed to eight quarters after regulatory approval, so that entities are not required to develop and maintain two sets of approved Critical Asset lists and Critical Cyber Asset lists concurrently. Requirements R1 and R2 were modified slightly to clarify that each list must be updated on an ongoing basis, but the review and approval need only occur annually. Conforming changes were made to the compliance section. Significant changes were also made to Attachment 1 to ten of the criteria. The criterion allowing entities to place items on the Critical Asset list at their discretion was deleted. The criterion for control centers was split into three criteria to allow for differentiation in size for Balancing Authorities and Transmission Operators. All of these changes were made in response to comments received.

In November of 2010, the Standards Committee Executive Committee authorized the standard drafting team to conduct an abbreviated comment period in parallel with a successive ballot, to support providing stakeholders with the opportunity to provide comment, while also supporting the goal of completing this set of revisions to CIP-002 before the end of December 2010. A successive ballot of the proposed CIP Version 4 Reliability Standards was conducted from December 1-10, 2010 and achieved a quorum of 86.83% and a weighted segment approval of 77.04%. Following this ballot, the Project 2008-06 drafting team made minor changes to the CIP-002-4 standard and the associated guidance document and implementation plan. A recirculation ballot was conducted from December 20-30, 2010 and achieved a quorum of 90.49% and a weighted segment approval of 80.56%.

The NERC Board of Trustees approved the proposed CIP Reliability Standards on January 24, 2011 and recommended they be added to the set of NERC Reliability Standards.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior 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

/s/ Holly A. Hawkins
Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

EXHIBITS A – F

(Available on the NERC Website at
http://www.nerc.com/fileUploads/File/Filings/Attachments_CIP_V4.pdf)