UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

VERSION 4 CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS	**Docket No. RM11-11-000**

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Willie L. Phillips
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
holly.hawkins@nerc.net
willie.phillips@nerc.net

November 21, 2011

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] hereby provides these comments in response to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking ("NOPR")[2] regarding the Version 4 Critical Infrastructure Protection ("CIP") Reliability Standards. In the NOPR, the Commission proposed to approve eight modified CIP Reliability Standards (CIP-002-4 through CIP-009-4), the accompanying Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") with modifications, the implementation plan, and the effective date developed and approved by NERC. The Commission seeks comments from interested parties on the proposed approval of the Version 4 CIP standards.

The purpose of the Version 4 CIP Reliability Standards is to provide a cybersecurity framework for the identification and protection of "Critical Cyber Assets" to support the reliable operation of the Bulk Power System.

By this filing, NERC submits its response to the NOPR.

[1] The Federal Energy Regulatory Commission ("FERC" or "Commission") certified NERC as the electric reliability organization ("ERO") in its order issued on July 20, 2006 in Docket No. RR06-1-000. *North American Electric Reliability Corporation*, "Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing," 116 FERC ¶ 61,062 (July 20, 2006).

[2] *Version 4 Critical Infrastructure Protection Reliability Standards, Notice of Proposed Rulemaking*, 136 FERC ¶ 61,184 (September 15, 2011) ("NOPR").

II. NOTICES AND COMMUNICATIONS

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

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Willie L. Phillips
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
holly.hawkins@nerc.net
willie.Phillips@nerc.net

III. DISCUSSION

A. The Proposed Reliability Standards

In a February 10, 2011 filing,[3] NERC requested Commission approval of the proposed Version 4 CIP Reliability Standards to replace the currently effective Version 3 CIP Reliability Standards. The Version 4 CIP Reliability Standards were developed in response to directives in Order No. 706[4] and propose to modify CIP-002-4 to include "bright line" criteria for the identification of Critical Assets, replacing the current entity-developed risk-based assessment methodology. NERC also developed conforming changes to the seven remaining Version 3 CIP Reliability Standards.

[3] *See Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection (CIP) Reliability Standards Version 4*, Docket No. RM011-11-000 (February 10, 2011) ("NERC Petition").
[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008).

NERC recognized in its original petition for approval that the Version 4 CIP Reliability Standards serve as an "interim step"[5] to addressing the complete set of directives in Order No. 706. NERC has not yet addressed all of the directives in Order No. 706 in the Version 4 CIP Reliability Standards but anticipates responding to all of the Order No. 706 directives in the Version 5 CIP Reliability Standards. The standard drafting team continues to develop solutions to the directives in a "phased" approach.

By this filing, NERC responds to the NOPR and urges the Commission to promptly approve the Version 4 CIP Reliability Standards.

B. Responses to Specific Matters Identified by the Commission

1. Whether Additional Critical Assets Can be Identified

In the NOPR, FERC is requesting comments on whether, under CIP Version 4, a responsible entity retains the flexibility to identify assets that, although outside of the bright line criteria, are essential to bulk power system reliability.[6] Additionally, FERC is requesting comments on whether NERC and/or the Regional Entities will have the ability, either in an event-driven investigation or compliance audit, to identify specific assets that fall outside the bright-line criteria yet are still essential to Bulk-Power System reliability and should be subject prospectively to compliance with the CIP standards.[7]

FERC is also requesting that NERC provide a method for review and approval of Critical Cyber Asset lists from external sources such as the Regional Entities or NERC.[8] FERC notes that the Regional Entities must have a role in the external review to ensure that there is sufficient

[5] NERC Petition at p. 6
[6] CIP V4 NOPR at P 31.
[7] *Id.*
[8] *Id.* at P 45.

accountability in the process and because the Regional Entities and NERC are ultimately responsible for ensuring compliance with Reliability Standards.[9] FERC states that, looking forward, it will be essential for NERC and the Regional Entities to actively review the designation of cyber assets that are subject to the CIP Reliability Standards, including those which span regions, in order to determine whether additional cyber assets should be protected.[10]

The proposed Version 4 CIP Reliability Standards present a bright-line for defining Critical Assets that provides certainty and clarity regarding those assets that should be identified as critical. In developing the proposed CIP-002-4 standard, the drafting team considered adding criteria that would allow entities to identify additional facilities falling outside of the bright-line criteria that they believe are essential to bulk power system reliability. Because of potential variances in application of additional facilities subject to the CIP standards, the drafting team made a determination not to add additional criteria beyond the bright-line criteria. However, responsible entities are permitted to apply any or all of the requirements in the CIP standards to assets that do not meet the bright-line thresholds.

The development of CIP Version 4 is an interim step to addressing all of the remaining Order No. 706 directives. The drafting team has used some post-version 4 information (*e.g.*, the results of the FERC-requested survey[11] and further industry discussions) to further refine the bright-line criteria with the intent to categorize assets as being of low, medium, or high impact that are "critical" to bulk power system reliability. NERC anticipates this will be reflected in the proposed CIP Version 5 standards scheduled to be filed for Commission approval in 2012.

[9] *Id.* at P 59.
[10] *Id.* at P 61.
[11] *See*, FERC's April 12, 2011 data request to NERC regarding the CIP V4 Reliability Standards, and NERC's May 27, 2011 response to the FERC data request, filed in FERC Docket No. Rm11-11-000.

In the interim period, if there are assets that NERC and the Regional Entities later determine should be treated as critical but do not meet the CIP Version 4 criteria, NERC has the authority under Section 810 of the NERC Rules of Procedure to issue a Level 2 (Recommendation) or Level 3 (Essential Action) Alert. Section 810 of the NERC Rules of Procedure provides the following:

> **810. Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions**
>
> 1. Members of NERC and bulk power system owners, operators, and users shall provide NERC with detailed and timely operating experience information and data.
> 2. In the normal course of operations, NERC disseminates the results of its events analysis findings, lessons learned and other analysis and information gathering to the industry. These findings, lessons learned and other information will be used to guide the reliability assessment program.
> 3. When NERC determines it is necessary to place the industry or segments of the industry on formal notice of its findings, analyses, and recommendations, NERC will provide such notification in the form of specific operations or equipment Advisories, Recommendations or Essential Actions:
>
>   3.1 Level 1 (Advisories) – purely informational, intended to advise certain segments of the owners, operators and users of the bulk power system of findings and lessons learned;
>
>   3.2 Level 2 (Recommendations) – specific actions that NERC is recommending be considered on a particular topic by certain segments of owners, operators, and users of the bulk power system according to each entity's facts and circumstances;
>
>   3.3 Level 3 (Essential Actions) – specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the bulk power system to take to ensure the reliability of the bulk power system. Such Essential Actions require NERC board approval before issuance.
>
> 4. The bulk power system owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) notifications apply are to evaluate and take appropriate action on such issuances by NERC. Such bulk power system owners, operators, and users shall also provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions in accordance with the reporting date(s) specified by NERC.
>
> 5. NERC will advise the Commission and other applicable governmental authorities of its intent to issue all Level 1 Advisories, Level 2 Recommendations, and Level 3

> Essential Actions at least five (5) business days prior to issuance, unless extraordinary circumstances exist that warrant issuance less than five (5) business days after such advice. NERC will file a report with the Commission and other applicable governmental authorities no later than thirty (30) days following the date by which NERC has requested the bulk power system owners, operators, and users to which a Level 2 Recommendation or Level 3 Essential Action issuance applies to provide reports of actions taken in response to the notification. NERC's report to the Commission and other applicable governmental authorities will describe the actions taken by the relevant owners, operators, and users of the bulk power system and the success of such actions taken in correcting any vulnerability or deficiency that was the subject of the notification, with appropriate protection for confidential or critical infrastructure information.

Level 3 Alerts, issued pursuant to NERC Rule of Procedure Section 810, allow NERC (following NERC Board of Trustees approval) to recommend that specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the bulk power system be taken to ensure the reliability of the bulk power system. Additionally, Rule 810 states that bulk power system owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) Alerts apply shall provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions consistent with reporting dates specified by NERC. Therefore, NERC can use Level 2 Recommendations and Level 3 Essential Actions as a tool to address assets that NERC and Regional Entities later determine should be treated as critical but do not fall into the CIP Version 4 criteria.

In Order No. 706-A,[12] FERC states "that oversight of a responsible entity's identification of critical cyber assets would occur at the compliance audit stage." The Version 4 standards work within that framework by providing the bright-line criteria for the identification of Critical Assets and providing for further oversight at the compliance audit stage.

[12] Order No. 706 at P. 50.

The Version 5 standards modify this approach by characterizing "BES Cyber Systems" as "High Impact," "Medium Impact," or "Low Impact" based on the impact of the cyber system to the reliable operation of the bulk power system. This characterization makes use of a bright-line concept similar to Version 4, but requires responsible entities to determine the impact of loss, compromise or misuse of a given BES Cyber System using a bright-line impact filter.

1. Whether the VSLs for CIP-002-4, Requirements R1 and R2 Should be Modified

In the NOPR, FERC expresses concern that the proposed Version 4 VSLs for CIP-002-4, Requirements R1 and R2 do not adequately address the purpose of NERC's proposed bright-line criteria: to ensure accurate and complete identification of all Critical Assets, so that all associated Critical Cyber Assets become subject to the protections required by the CIP Standards.[13] FERC states that neither set of VSLs address the failure to properly identify either Critical Assets or Critical Cyber Assets in the first place.[14] FERC therefore proposes to direct NERC to modify the VSLs for CIP-002-4, Requirements R1 and R2, to address a failure to identify either Critical Assets or Critical Cyber Assets, as shown in Appendix 1 of the NOPR.[15]

NERC agrees with FERC that the VSLs for CIP-002-4, Requirements R1 and R2 should be modified, and proposes to add the word "complete" in the front of the list in the VSL language to ensure that the list of identified Critical Assets from each Responsible Entity is a complete list. The new language would read as follows: "The Responsible Entity did not

[13] NOPR at P 35.
[14] *Id.* at P 36.
[15] *Id.* at P 37.

develop a complete list of its identified Critical Assets even if such list is null." This would keep the requirements binary, consistent with FERC's guidance on this issue.[16]

In order to modify the VSLs for CIP-002-4, Requirements R1 and R2, NERC will have to conduct a non-binding poll, present the proposed changes to the NERC Board of Trustees for approval, and then file the proposed changes with FERC for approval, which could take NERC several months to complete.

2. Proposed CIP Version 4 Implementation Plan

In the NOPR, FERC proposes to approve the proposed Implementation Plan for CIP V4 as filed.[17]

NERC agrees with FERC's proposal to approve the proposed Implementation Plan for the Version 4 CIP Reliability Standards as filed.

3. Deadline to Respond to Order No. 706 Directives

FERC is proposing in the NOPR to direct NERC to submit modified CIP Reliability Standards that address the outstanding directives from Order No. 706, using NERC's development timeline included in the petition.[18] This timeline specifies that NERC submit a modified set of CIP Reliability Standards to the NERC Board for approval by the end of second quarter 2012, and file with FERC by the end of third quarter 2012.[19]

NERC appreciates FERC's acknowledgement that Version 4 is an interim step in addressing outstanding directives from Order No. 706, and is working to develop the CIP Version 5 Reliability Standards by the timeline NERC proposed in the petition. As long as a

[16] *See, Mandatory Reliability Standards for Critical Infrastructure Protection, Order Addressing Violation Severity Level Assignments for Critical Infrastructure Protection Reliability Standards,* 130 FERC ¶61,211, at P 14 (March 18, 2011).
[17] NOPR at PP 38-39.
[18] *Id.* at P 41.
[19] *Id.* at PP 41, 66-67.

FERC Order on the CIP Version 4 standards does not add to or expand directives from Order No. 706 or include directives that add to that timeline, the proposed deadline to file the Version 5 standards by third quarter 2012 is acceptable to NERC, subject to the discussion that follows. A FERC Order must be conditioned upon NERC's use of the FERC-approved standards development process as implemented, which requires industry approval and NERC Board of Trustees approval, before filing with FERC.

FERC is correct that, under the timeline to address all outstanding Order No. 706 directives, NERC anticipates a filing of Version 5 with FERC by the end of the third quarter of 2012. These projected timelines for standards development projects are routinely prepared to assist in resource planning within its standards development process, and by general practice, they do not include more than one successive ballot period

A 60-day initial posting period for formal comment and initial ballot of the Version 5 CIP Reliability Standards began November 7, 2011, and ends on January 6, 2012. In recognition of the volume of standards requirements and the scope of changes in Version 5 from Version 4, that posting period is longer than the more common 45-day initial posting period for formal comment. A second formal posting for comment and successive ballot period is scheduled to begin on March 26, 2012. However, the timing of that formal posting and successive ballot period depends on the number of industry comments received in response to the November 7 posting and the number of changes that may need to be made to the language in the standards as a result of those comments. In the event there is strong stakeholder opposition to the proposed standards, resulting in a failed ballot of any or all of the Version 5 CIP standards, NERC may not be able to file the Version 5 CIP standards by the third quarter 2012. Even though the drafting team has removed standard-to-standard dependencies in Version 5, the Version 5 standards must

be filed together because they collectively represent a significant change from previous versions. While NERC will make every effort to address stakeholder concerns before the successive ballot, the nature of the standards development process, and ultimately a favorable outcome on the proposed standards, is in the hands of the registered ballot body, which will in turn, affect the final delivery of the proposed CIP Version 5 standards to FERC for approval.

Thus, if a deadline must be established, NERC urges FERC to consider that a filing resulting from the FERC-approved standards development process by the end of the third quarter 2012 is only possible if the implementation of the standards development process requires only one successive ballot.

NERC notes that its anticipated timeline to file the Version 5 CIP Standards, in conjunction with the Implementation Plan proposed in the initial draft of Version 5, may present the opportunity to suggest an extension of Version 3 until Version 5 can be implemented, thereby eliminating the need for implementing Version 4, to be followed only a short time later by implementation of Version 5. That suggestion is not being made now, and it could be considered only if the industry moves promptly on Version 5. If Version 5 is not approved by the industry, filed by NERC, and approved by the Commission within that anticipated schedule, or reasonably thereafter, it is unlikely that Version 3 could be extended in a manner that eliminates the need for implementation of Version 4.

4. Identification of Critical Cyber Assets Based Upon a Cyber Asset's Connectivity and Potential to Compromise the Reliable Operation of the Bulk Power System

In the NOPR, FERC states that, in light of recent cybersecurity vulnerabilities and threats and attacks that have exploited the interconnectivity of cyber system, FERC is seeking comments regarding the method of identification of Critical Cyber Assets to ensure sufficiency and

accuracy.[20] FERC states that it believes that any criteria adopted for the purposes of identifying a Critical Cyber Asset under CIP-002 should be based upon a Cyber Asset's connectivity and its potential to compromise the reliable operation of the bulk power system, rather than focusing on the operation of any specific Critical Assets.[21] FERC is requesting comments on this approach.[22]

The Version 5CIP Reliability Standards drafting team is aware of recent cybersecurity vulnerabilities that may have the potential to exploit the interconnectivity of cyber systems. While the Version 5 CIP Reliability Standards drafting team recognizes the importance of the connectivity issue and is looking at this in the development of the Version 5 standards, this issue was not raised in FERC's Order No. 706. The drafting team is assessing FERC's suggested approach. However, it is unlikely that this work can be completed before the Version 5 CIP Reliability Standards are presented to the NERC Board of Trustees for approval.

Importantly, the proposed Version 5 CIP Reliability Standards remove the blanket exemption for non-routably connected cyber systems, and instead move the connectivity attribute to specific requirements. Additionally, the draft standard proposes to apply electronic perimeter protections of some form to all BES Cyber Systems.

5. NIST Risk Management Framework

FERC is requesting comments on whether NERC should consider applicable features of the National Institute of Standards and Technology (NIST) Risk Management Framework to ensure protection of all cyber systems connected to the bulk power system, including

[20] *Id.* at P 43.
[21] *Id.*
[22] *Id.*

establishing CIP requirements based on entity functional characteristics rather than focusing on Critical Asset size.[23]

In Paragraph 25 of Order No. 706, the Commission stated:

> 25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

Consistent with this direction, NERC is considering applicable features of the NIST Risk Management Framework in the development of the Version 5 CIP Reliability Standards. One of the fundamental differences between CIP Version 4 and CIP Version 5 is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change resulted from the standard drafting team's review of the NIST Risk Management Framework and the use of an analogous term of "information system" as the target for categorizing and applying security controls.

However, although the standard drafting team is considering changes in the Version 5 CIP Reliability Standards that are reflective of the NIST Risk Management Framework, it is important to highlight differences between NERC's and NIST's approaches. At the root of these differences are divergent responsibilities and goals between NERC and NIST. NIST develops standards and guidance for U.S. Federal Agencies to manage risks to their information and systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to prevent or protect against in order to achieve the

[23] *Id.* at PP 45-52.

reliability of the BES. In contrast, NIST is developing standards for almost two hundred different organizations, each with vastly different missions. The advantage of the NERC standards is a focus on a relatively small number of reliability services that need to be protected. This ultimately means that the NERC standards can be more tailored to the industry than a wholesale adoption of the NIST Risk Management Framework.

Four key features of the NIST Risk Management Framework were incorporated into the proposed CIP Version 5 Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk-Power System, based on their function and impact, receive some level of protection; (2) customizing protection to the mission of the cyber systems subject to protection; (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk-Power System; and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled.

The criteria defined in Attachment 1 of the proposed CIP-002-5 standard are used to categorize BES Cyber Systems and their BES Cyber Assets into impact categories, resulting in all BES Cyber Systems and BES Cyber Assets being included in scope. Requirement R1 only requires the discrete identification of BES Cyber Systems and BES Cyber Assets for those in the "High" and "Medium" categories. All other BES Cyber Systems are deemed to be "Low" impact. This general process of categorization of BES Cyber Systems and BES Cyber Assets based on impact to the reliability of the BES is consistent with risk management approaches for the purpose of application of cyber security controls in the rest of the Version 5 CIP standards.

In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to its specific environment and make modifications to those controls. However, in the NERC compliance

framework, all requirements are mandatory and enforceable. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of bulk power system reliability.

While it may appear that the standard drafting team's approach to categorization is based on an asset's "size," in reality, the characterization is based on the "impact" of a misuse or compromise, or of the scope of control, of the BES Cyber System. Additionally, because electronic perimeter protections are now required surrounding all BES Cyber Systems (with specific requirements for High Impact, Medium Impact, and programmatic requirements for Low Impact), the connectivity issue FERC discussed in the NOPR should be largely addressed.

6. Potentially Unprotected Control Centers

In the NOPR, FERC expresses concern that the proposed CIP-002-4 bright line criteria do not adequately address FERC's Order No. 706 directive regarding the classification of control centers or take the potential misuse of control systems into account in the identification of Critical Assets.[24] FERC states as an example that the proposed bright line criteria leave a number of Critical Assets with potentially unprotected cyber assets, including a total of 222 control centers, with no legal obligation to apply cybersecurity measures.[25] FERC states that these potentially unprotected control centers involve an unknown number of associated control systems, and that therefore "[i]t is critical…that the Commission's concerns regarding the

[24] *Id.* at 56.
[25] *Id.*

potential misuse of control centers and associated control systems be addressed in the CIP Reliability Standards." [26]

Under the Version 5 CIP Reliability Standards, every control center will be covered by either the "Medium" or "High" criteria, which requires a greater level of protection. Because of their impact and size, no control center will qualify under the "Low" criteria. Version 5 also includes a responsibility entity's consideration of cyber misuse as part of its BES Cyber System classification. Furthermore, several of the Version 5 standards' requirements are specifically made applicable to not only "High" impact BES Cyber Systems, but also to "Medium" impact BES Cyber Systems at Control Centers. Through the use of both classification and applicability, certain requirements apply to all Control Centers, regardless of classification.

Additionally, there is not a universally accepted definition of "control center" (although the Version 5 CIP Reliability Standards drafting team has proposed one). However, by the current working definition, particularly for generation, some "control centers" have a span of control that is below the NERC Registration criteria for generators (*i.e.*, 20 MVA unit, 75 MVA plant) that only communicate with the other generators within its control. Therefore, it is difficult to imagine scenarios where cyber assets at these locations have a greater impact to reliability, simply because they meet the definition of "control center," than much larger, single-unit generators that do not meet the bright-line criteria for medium impact.

IV. CONCLUSION

For the reasons stated above, NERC respectfully requests that the Commission take prompt action in approving the proposed Version 4 CIP Reliability Standards consistent with these comments when it issues its Final Rule in this proceeding.

[26] *Id.* at PP 56, 58.

Respectfully submitted,

/s/ Holly A. Hawkins

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Willie L. Phillips
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
holly.hawkins@nerc.net
willie.phillips@nerc.net

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 21st day of November, 2011.

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric Reliability Corporation