NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

November 29, 2016

VIA ELECTRONIC FILING

David Erickson
President and Chief Executive Officer
Alberta Electric System Operator
2500, 330 - 5 Avenue SW
Calgary, Alberta
T2P 0L4

RE: *North American Electric Reliability Corporation*

Dear Mr. Erickson:

The North American Electric Reliability Corporation hereby submits Notice of Filing of the North American Electric Reliability Corporation of Interpretation of Proposed Reliability Standard CIP-002-5.1a. NERC requests, to the extent necessary, a waiver of any applicable filing requirements with respect to this filing.

NERC understands the AESO may adopt the proposed reliability standards subject to Alberta legislation, principally as established in the *Transmission Regulation* ("the T Reg."). Briefly, it is NERC's understanding that the T Reg. requires the following with regard to the adoption in Alberta of a NERC Reliability Standard:

1. The AESO must consult with those market participants that it considers are likely to be directly affected.

2. The AESO must forward the proposed reliability standards to the Alberta Utilities Commission for review, along with the AESO's recommendation that the Commission approve or reject them.

3. The Commission must follow the recommendation of the AESO that the Commission approve or reject the proposed reliability standards unless an interested person satisfies the Commission that the AESO's recommendation is "technically deficient" or "not in the public interest."

Further, NERC has been advised by the AESO that the AESO practice with respect to the adoption of a NERC Reliability Standard includes a review of the NERC Reliability Standard for applicability to Alberta legislation and electric industry practice. NERC has been advised that, while the objective is to adhere as closely as possible to the requirements of the NERC Reliability Standard, each NERC Reliability Standard

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

approved in Alberta (called an "Alberta reliability standard") generally varies from the similar and related NERC Reliability Standard.

NERC requests the AESO consider the interpretation of Proposed Reliability Standard CIP-002-5.1a in the filing for adoption in Alberta as an "Alberta reliability standard(s)," subject to the required procedures and legislation of Alberta.

Please contact the undersigned if you have any questions concerning this filing.

Respectfully submitted,

/s/ Shamai Elstein

Shamai Elstein
Senior Counsel for the North American Electric Reliability Corporation

Enclosure

BEFORE THE
ALBERTA ELECTRIC SYSTEM OPERATOR

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

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF INTERPRETATION OF RELIABILITY STANDARD CIP-002-5.1a

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
charles.berardesco@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

November 29, 2016

TABLE OF CONTENTS

BEFORE THE
ALBERTA ELECTRIC SYSTEM OPERATOR

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION)
)

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF INTERPRETATION OF RELIABILITY STANDARD CIP-002-5.1

The North American Electric Reliability Corporation ("NERC") hereby submits a proposed interpretation of Reliability Standard CIP-002-5.1. The proposed interpretation provides clarification regarding the meaning of the phrase "shared BES Cyber Systems" in Criterion 2.1 of Attachment to Reliability Standard CIP-002-5.1.[1] As discussed further below, the proposed interpretation provides that: (1) the phrase "shared BES Cyber Systems" in Criterion 2.1 refers to discrete BES Cyber Systems that are shared by multiple generation units; and (2) the evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System.

The proposed interpretation appended to CIP-002-5.1a (**Exhibit A**) is just, reasonable, not unduly discriminatory or preferential, and in the public interest.[2]

This filing presents the technical basis and purpose of the proposed interpretation and the complete record of development (**Exhibit B**). The proposed interpretation was adopted by the NERC Board of Trustees on November 2, 2016.

---

[1] Unless otherwise designated, capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("*NERC Glossary*"), *available at* http://www.nerc.com/files/Glossary_of_Terms.pdf.

[2] Consistent with NERC numbering convention, the standard number would be CIP-002-5.1a.

I. NOTICES AND COMMUNICATIONS

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

Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
shamai.elstein@nerc.net

II. BACKGROUND

A. Interpretation Procedural History

NERC submitted Reliability Standard CIP-002-5 on February 7, 2013 and submitted an Errata on October 4, 2013 (CIP-002-5.1). FERC approved CIP-002-5.1 in Order No. 791, issued on November 22, 2013.[3] On March 3, 2015, as amended on May 8, 2015, Energy Sector Security Consortium, Inc. ("EnergySec") filed a Request for Interpretation ("RFI") of Reliability Standard CIP-002-5.1 seeking clarification regarding the use of the phrase "shared BES Cyber Systems" in Criterion 2.1 of Attachment 1 to the standard. The NERC Standards Committee accepted the RFI on September 23, 2015 and directed the existing standard drafting team working on revisions to the CIP Reliability Standards to act as the interpretation drafting team for purposes of the EnergySec RFI.

The proposed interpretation was posted for a 45-day comment period and ballot, ending on September 12, 2016. The proposed interpretation achieved a 75.43% quorum and 91.68%

[3] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and rehearing*, Order No. 791-A, 146 FERC ¶ 61, 188 (2014).

approval from stakeholders. Pursuant to the NERC Rules of Procedure, the proposed interpretation was posted for a 10-day final ballot from October 13, 2016 through October 24, 2016, resulting in a 81.25% quorum and 91.31% approval. The proposed interpretation was approved by the NERC Board of Trustees on November 2, 2016.

III. JUSTIFICATION

The purpose of Reliability Standard CIP-002-5.1 is to identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the Bulk Electric System. Attachment 1 to the standard sets forth the criteria used to categorize BES Cyber Systems into impact categories (i.e., high, medium or low impact). The proposed interpretation provides clarity regarding the application of Criterion 2.1 of Attachment 1. The proposed interpretation is just, reasonable, not unduly discriminatory or preferential, and in the public interest.

A. EnergySec RFI of Criterion 2.1 of Attachment 1 to CIP-002-5.1

Criterion 2.1 of Attachment 1 provides that BES Cyber Systems associated with the following should be categorized as medium impact:

> Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

EnergySec's RFI posed the following questions with respect to the meaning of the phrase "shared BES Cyber Systems" in the second sentence of Criterion 2.1:

1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

B. Proposed Interpretation

In response to the EnergySec RFI, Reliability Standard CIP-002-5.1a adds an interpretation as Appendix 1 to the standard that clarifies that: (1) the phrase "shared BES Cyber Systems" in Criterion 2.1 refers to discrete BES Cyber Systems that are shared by multiple generation units; and (2) the evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. The proposed interpretation thus incorporates, into the standard document, the explanation that an entity must separately evaluate each BES Cyber System under Criterion 2.1 to determine whether the BES Cyber System is shared by – i.e., used by or could affect – more than one unit at a generating plant.

Specifically, in response to the first question posed by EnergySec, the proposed interpretation provides as follows:

> The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*… associated with any of the following [criteria]." (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

In response to the second question, the proposed interpretation clarifies that "[t]he phrase 'shared BES Cyber Systems' refers to discrete BES Cyber Systems that are shared by multiple generation units." The proposed interpretation also notes that NERC's Frequently Asked Questions document issued to support implementation of the CIP Reliability Standards approved in FERC Order No. 791 (the "CIP FAQs") also address the meaning of the phrase "shared BES Cyber System."[4] Specifically, the proposed interpretation cites FAQ #49, which provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR." Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: Impact Rating of Generation Resource Shared BES Cyber Systems for further information and examples.[5]

---

[4] The CIP FAQs are available at http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPV5_FAQs_Consolidated_Oct2015_Oct_13_2015.pdf.

[5] CIP FAQs at 2.

In short, the interpretation clarifies that a "shared BES Cyber System" under Criterion 2.1 is a BES Cyber System that, if rendered unavailable, degraded, or misused, could affect the operation of more than one unit at a generation plant. As explained in the NERC Lesson Learned document referenced in FAQ #49, "[i]dentifying shared BES Cyber Systems involves detailed analysis that considers shared generating plant operational processes (e.g., air, water, steam, environmental, and fuel handling processes) and electronic connectivity."

As the proposed interpretation clarifies that the phrase "shared BES Cyber Systems" applies to each discrete BES Cyber System, not collectively to groups of BES Cyber Systems, the third question in the RFI is moot.

Respectfully submitted,

/s/ Shamai Elstein

Charles A. Berardesco
Senior Vice President and General Counsel
Shamai Elstein
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
charles.berardesco@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

November 29, 2016

EXHIBITS A —C