UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Systems in Control Centers	**)**	**Docket No. RM16-18-000**

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

The North American Electric Reliability Corporation ("NERC") hereby provides comments on the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Inquiry ("NOI") seeking comment on the need for, and possible effects of, modifications to the Critical Infrastructure Protection ("CIP") Reliability Standards regarding the cybersecurity of Control Centers used to monitor and control the bulk electric system in real time.[1] Specifically, the Commission "seeks comment on possible modifications to the CIP Reliability Standards – and any potential impacts on the operation of the Bulk-Power System ("BPS") resulting from such modifications – to address the following matters: (1) separation between the Internet and BES Cyber Systems in Control Centers performing transmission operator functions; and (2) computer administration practices that prevent unauthorized programs from running, referred to as "application whitelisting," for cyber systems in Control Centers."[2]

NERC supports continued focus on protecting cyber systems in Control Centers, particularly in view of the 2015 cyberattack in Ukraine that targeted the control systems of three electric power distribution companies. Cybersecurity threats pose a serious, evolving, and ongoing challenge for the electricity subsector. NERC has existing mandatory CIP Reliability Standards

[1] Notice of Inquiry, *Cyber Systems in Control Centers*, 156 FERC ¶ 61,051, 81 Fed. Reg. 49641 (2016).

[2] *Id*. at P 2.

that, among other things, are designed to mitigate Internet borne threats and the risks associated with malicious code. In complying with these Reliability Standards, entities may choose to isolate their BES Cyber Systems in Control Centers from the Internet and use application whitelisting technologies, as they deem necessary and appropriate from both a security and operational perspective. As with all of its Reliability Standards, NERC continually evaluates whether modifications to the CIP Reliability Standards are necessary to provide for a more secure and reliable BPS in North America. NERC appreciates the Commission's continued efforts to facilitate discussion on potential enhancements to NERC's CIP Reliability Standards.

In its comments below, NERC discusses the potential benefits and drawbacks to requiring the additional protections discussed in the NOI. As discussed below, while these protections may help reduce cybersecurity threats and vulnerabilities, mandating such prescriptive controls may also unduly limit operational flexibility without proportionate reliability benefit. NERC must further evaluate the impact of those protections on operations to understand when and how those protections could be implemented without undue interference with the operational needs of Responsible Entities.

NERC respectfully requests that the Commission not direct modifications to the CIP Reliability Standards at this time to provide NERC additional time to more comprehensively evaluate the need for and potential drawbacks to mandating Internet isolation and application whitelisting. As NERC (1) evaluates the manner in which entities implement the controls required in the currently-effective CIP Reliability Standards and the effectiveness of those controls in mitigating cybersecurity risks to the BPS, (2) conducts the study on remote access protections, as

directed in Order No. 822,[3] and (3) modifies the Reliability Standards consistent with directives from Order Nos. 822 and 829,[4] NERC should have a better understanding as to whether additional, more prescriptive controls like those discussed in the NOI are necessary and the potential implications of such controls on operations.

Further, additional directives at this time would increase an already significant workload for NERC and industry with respect to implementation of, and development of modifications to, the CIP Reliability Standards. As discussed below, significant industry resources are currently devoted to implementation of the CIP Reliability Standards, both those Requirements applicable to high and medium impact BES Cyber Systems, which only went into effect on July 1, 2016, and those Requirements applicable to low impact BES Cyber System, whose implementation is not required until April 1, 2017. Additionally, NERC and industry resources are currently devoted to addressing Commission directives from Order Nos. 822 and 829 as well as modifications to the CIP Reliability Standards to address issues identified during implementation.

I. COMMENTS

a. Potential Benefits and Impact of Requiring Internet Isolation

As noted above, the Commission seeks comment on whether the CIP Reliability Standards should be modified to require isolation between the Internet and BES Cyber Systems in Control Centers performing the functions of a transmission operator.[5] The Commission also seeks comment on the operational impact to the BPS if BES Cyber Systems were isolated from the

[3] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037 at PP 3, 18, 64 (2016).

[4] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016).

[5] NOI at P 11.

Internet in all Control Centers performing transmission operator functions.[6] The following is a discussion on NERC's perspectives on the benefits and potential operational impact of mandating Internet isolation at Control Centers performing the functions of a Transmission Operator.

i. Reliability Benefits

As the Commission recognizes in the NOI, the reliability benefit of isolating BES Cyber Systems from the Internet is that such isolation helps reduce Internet borne threats. The Internet serves as one of the more commonly used attack vectors for perpetrating a cyberattack, whether as a path by which a malicious actor gains access to a computer or network server to deliver a payload or malicious outcome, or by exploiting system vulnerabilities, including the human element. If an entity allows only data connections to Control Centers or other facilities owned by Transmission Operators over dedicated data lines owned or leased by the Transmission Operator, rather than allowing communications over the Internet, it could limit the number of ways that malicious actors could access BES Cyber Systems. As such, separating BES Cyber Systems from the Internet may strengthen and simplify an entities cybersecurity activities.

As the Commission noted, the CIP Reliability Standards do not currently mandate that entities isolate their BES Cyber Systems in Control Centers performing transmission operations from the Internet. The risk-based framework established in the CIP Reliability Standards seeks to balance the operational needs of responsible entities to have Internet connections to BES Cyber Systems in Control Centers with the security need to protect against Internet borne threats. To accommodate Responsible Entity operational needs for Internet connectivity within their Control Centers, discussed below, the CIP Reliability Standards permit BES Cyber Systems to route, or

6 *Id.*

connect, to the Internet while requiring Responsible Entities to limit, manage, and control Internet connectivity to protect against Internet borne threats.

Specifically, the CIP Reliability Standards include a number of Requirements designed to mitigate the risks associated with Internet connectivity, including the following examples:

- *CIP-005-5, Requirement R1* requires entities to establish an Electronic Security Perimeter ("ESP") to control electronic access to BES Cyber Systems. An ESP is the "logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." Among other things, Requirement R1 specifies that (1) all External Routable Connectivity, such as Internet connections, must go through an Electronic Access Point ("EAP") that requires inbound and outbound access permissions based on a valid need for granting such access; and (2) each EAP has one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

- *CIP-005-5, Requirement R2* addresses the protections required for Interactive Remote Access, which is defined as "[u]ser access by a person employing a remote access client or other remote access technology using a routable protocol." Requirement R2 mitigates the risks of remote access through the Internet by requiring that entities (1) use an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset; (2) use encryption that terminates at an Intermediate System; and (3) require multi-factor authentication for all Interactive Remote Access sessions. These remote access protections would significantly impair a malicious actor's attempts to perpetrate the type of cyberattack carried out in the Ukraine referenced in the NOI.

- *CIP-007-6, Requirement R1* requires entities to (1) enable only logical network accessible ports that have been determined to be needed by the Responsible Entity; and (2) protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. The controls help reduce the attack surface of Cyber Assets.

- *CIP-007-6, Requirement R2* requires entities to implement a patch management process for tracking, evaluating, and installing cybersecurity patches. This security control helps ensure that entities fix known software vulnerabilities that could be exploited by a malicious actor through the Internet.

- *CIP-007-6, Requirement R3* requires entities to (1) deploy methods to detect, deter, or prevent malicious code, and (2) mitigate the threat of detected malicious code. This requirement helps prevent and mitigate the threat of malicious code that may be introduced through Internet connections.

In complying with these Requirements, entities may choose to isolate some or all of their BES Cyber Systems from the Internet as they deem necessary and appropriate from both a security

and operational perspective. Mandating such isolation to all BES Cyber Systems in a Control Center performing transmission operations, however, could impact operations without proportionate reliability benefit, as discussed below.

ii. Operational Impacts

As the Commission recognizes in the NOI, any added security benefit from Internet isolation must also be weighed against operational impact. Mandating complete Internet isolation for BES Cyber Systems in Control Centers performing transmission operator functions may not be feasible as it could impact, among other things, data exchange, remote access, patch management, and transmission scheduling capabilities, each of which is discussed in turn, below:

Data exchange capabilities: NERC understands that certain Transmission Operators already use dedicated data lines for communication between their Control Center and those of other functional entities. Nevertheless, Transmission Operators rely on the Internet to exchange a significant amount of data with other functional entities, particularly small entities performing generation, transmission, balancing, and interchange functions. Requiring all such data exchanges to occur over dedicated lines owned or leased by the Transmission Operator could have significant cost implications. As reliable operations depend on the free flow of data between various functional entities, a costly security measure could unintentionally limit necessary and timely data exchange.

Entities also rely on Internet connections for data exchange between BES Cyber Systems and their corporate networks. Some of these data exchanges may be for the express purpose of enhancing cyber and physical security management through the organization. For instance, an entity may implement a corporate Identity Management System, or to correlate security events across the enterprise using a corporate Security Information and Event Management system. An entity may also use a corporate Active Directory and secure authentication appliances. Requiring

complete Internet isolation would also require the reconfiguration of data connections between BES Cyber Systems and corporate networks.

Remote Access Capabilities: Remote access for management and support of BES Cyber Systems generally necessitates access over the Internet. Many entities rely on Internet connections to provide for remote access, both to allow its own employees to have remote operational capabilities and for vendor operational support. Complete isolation from the Internet would preclude many entities from providing for such remote access as using dedicated lines for these purposes is impractical and could have significant cost implications. Remote vendor support is most economically provided via Internet connections. Leasing or owning dedicated networks would likely involve significant new costs and may be too expensive for some smaller entities. It may not be practical to establish a point-to-point private high-speed network from each vendor to the Control Center networks.

While precluding the use of remote access may increase security by limiting points of access to carry out a cyberattack, it could also potentially reduce reliability by increasing response time for resolving operational issues. From an operations perspective, it may not be feasible to mandate 24x7 onsite support in order to remove the requirement for remote access, nor may it be feasible to mandate that entity staff or vendor personnel come into the Control Center to provide break-fix support, delaying the return of a failed Cyber Asset to operation. If a system necessary for reliable operations malfunctions and Control Center personnel present at the time of the malfunction do not have the ability to address the malfunction, remote support, from other Responsible Entity personnel or a vendor, could quickly resolve the issue. Absent such remote access capability, the individuals with the capability to resolve the issue would have to be physically present to address the issue, which may not always be able to be accomplished on a

timely basis, particularly if access by a remote vendor in another geographic region is required to diagnose the problem. Remote access provides Responsible Entities with a means to obtain rapid response capabilities that, in some situations and for some entities, is an important reliability and security need.

Patch Management: Pursuant to Reliability Standard CIP-007-6, Requirement R2, entities must have a patch management process to track, evaluate, and install cyber security patches to mitigate the risks associated with software vulnerabilities. Vendor patches are often available only via the Internet. Complete isolation from the Internet could thus affect entities' patch management processes, creating challenges for installing patches to address software vulnerabilities.

Transmission Scheduling Capabilities: Another operational issue to consider is the need to have an Internet connection to cyber systems in Control Centers used for transmission scheduling purposes. The primary means by which transmission service is scheduled in North America is through the Open Access Same-Time Information System ("OASIS"), an Internet-based system mandated by FERC and managed primarily by OATI, Inc. Transmission Operators require real-time access to OASIS systems to provide updated Available Transmission Capacity and Total Transmission Capacity values for use by the OASIS reservation system, and real-time access to transactions made in the OASIS system to perform congestion analysis. Requiring Internet isolation would create challenges for entities that rely on OASIS to schedule transmission service. There may be other market systems for the purchase, sale, or transmission of power that rely on Internet connection to and from a Control Center that could also be affected.

Given the potential for Internet isolation to have operational impacts, any requirement mandating such isolation must be carefully considered and narrowly tailored to take advantage of the security benefits without causing undue operational difficulties. As discussed further below,

NERC respectfully requests that the Commission not issue any directives at this time to allow NERC to further evaluate the need for such protections, particularly in light of the directives in Order Nos. 822 and 829, and understand when and how Internet isolation could be implemented without undue interference with the operational needs of Responsible Entities.

b. Potential Benefits and Impact of Requiring Application Whitelisting

In addition to Internet isolation, the Commission seeks comment on whether the CIP Reliability Standards should be modified to require application whitelisting for all BES Cyber Systems in Control Centers. As discussed below, using application whitelisting is one approach to meeting the objective of Reliability Standard CIP-007-6, Requirement R3, which requires Responsible Entities to mitigate malicious cyber activity. The following is a discussion of the benefits and potential operational impact of mandating the use of application whitelisting for all BES Cyber Systems in Control Centers.

i. Reliability Benefits

Application whitelisting technologies are intended to stop the execution of malicious code and other unauthorized software and are an effective solution to mitigating risks associated with sophisticated malware, Advanced Persistent Threat, and Zero-day attacks. As the Commission stated in the NOI, "application whitelisting is a computer administration practice used to prevent unauthorized program from running…to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for computer resources."[7] An application whitelist is essentially a list of applications and application components (libraries, configuration files, etc.) that are authorized for use in an organization (organization-wide or on a

[7] NOI at P 12.

particular system). Based on the application whitelist, technologies or programs are used to control which applications are permitted to be installed or executed.

Application whitelisting technologies thus provide straightforward and significant protection – i.e., code that is not permitted to run on a system, is prevented from running. "Unlike security technologies such as antivirus software, which block known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other."[8] Application whitelisting is most effective in environments, like utility control systems, where application diversity and change is minimal. The maintenance of the whitelist over time as applications and the organization's needs change is vital to ensuring that the application whitelisting technologies provide the necessary protections without unduly limiting operational needs.

As the NOI notes, application whitelisting is one approach to meeting the objective of Reliability Standard CIP-007-6, Requirement R3, which requires Responsible Entities to mitigate malicious cyber activity. Specifically, CIP-007-6, Requirement R3 requires entities to (1) deploy methods to detect, deter, or prevent malicious code, and (2) mitigate the threat of any detected malicious code. When implemented correctly, application whitelisting is an effective preventative measure that entities may use to comply with the Requirement. As an effective preventative control, it may also be more protective than controls designed only to mitigate the risks associated with malicious code detected on the BES Cyber Systems.

Recognizing the diversity of BES Cyber Systems and the environments in which they are used across the BPS, however, the mandatory CIP Reliability Standards provide entities the

[8] *See* National Institute of Standards and Technology Special Publication 800-167, Guide to Application Whitelisting, at P 5, *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

flexibility to employ a variety of methods, based on the needs and characteristics of their systems, to meet the objective of mitigating malicious cyber activity. The risk-based framework of the CIP Reliability Standards is designed to require entities to meet a security objective without specifically prescribing the manner in which entities must meet that objective in every instance. Although, under certain circumstances, application whitelisting may be a more effective mitigation tool than other available options, it may not be appropriate or provide added reliability benefit in every instance. Prescribing the use of application whitelisting for every BES Cyber System may have unintended operational consequences, as discussed below.

ii. Operational Impact

As with Internet isolation, the reliability benefits of application whitelisting must be weighed against the operational impact of implementing such a prescriptive control. Specifically, there should be consideration of the following issues when evaluating the use of application whitelisting:

1) Whether implementing application whitelisting technologies on a vendor supplied and supported product would create any issues with future vendor support. Vendors may not allow for the installation of non-supported software on their products.

2) Application whitelisting technologies are not "plug-and-play" and may require extensive testing before effective implementation.

3) Use of application whitelisting would require updates to change management and patch installation processes to accommodate application whitelisting technologies.

4) Application whitelisting could have the unintended consequence of preventing timely execution of essential programs which have benign modifications. For instance, to properly use application whitelisting, systems must be baselined to identify all permitted application software. Baselining is a difficult task, especially when certain software might only run under abnormal conditions. If the baseline is not 100% accurate and complete, critical software could be prevented from executing at a most critical time.

5) Application whitelisting technology may not be available on all equipment or architectures.

As with Internet isolation, mandating application whitelisting presents certain challenges and must be carefully considered and narrowly tailored to apply in those instances where the security benefits may be realized without causing undue operational difficulties. Moreover, while application whitelisting appears to be a leading-edge technology at this time, that may not be the case in the future. Mandating application whitelisting may preclude use of other technologies proven to be technically superior, which is counter to the results-based framework established in the current CIP Reliability Standards. For these reasons and as discussed further below, NERC respectfully requests that the Commission not issue any directives at this time to allow NERC to further evaluate the need for application whitelisting, and understand when and how those protections could be implemented without undue interference with the operational needs of Responsible Entities.

c. The Commission Should Not Direct Modifications to the CIP Standards at this Time

For the reasons outlined below, there needs to be additional time to evaluate the need for and potential drawbacks to mandating Internet isolation and application whitelisting as contemplated in the NOI. As NERC (1) evaluates the manner in which entities implement the controls required in the currently-effective CIP Reliability Standards and the effectiveness of those controls, (2) conducts the study on remote access protections, as directed in Order No. 822, and (3) modifies the Reliability Standards consistent with directives from Order Nos. 822 and 829, NERC will have a better understanding as to whether additional, more prescriptive controls like those discussed in the NOI are necessary and the potential implications of such controls on operations.

As the Commission recognized in the NOI and as discussed above, the CIP Reliability Standards include a number of Requirements designed to mitigate the risks that Internet isolation

and application whitelisting are also intended to mitigate.[9] These Requirements are risk based and results based, providing responsible entities the flexibility to implement security controls consistent with their business and operational needs and to take advantage of emerging technologies. As the Requirements for high and medium impact BES Cyber Systems only became effective on July 1, 2016,[10] the Commission should allow responsible entities time to implement the currently-approved controls before mandating the use of the more prescriptive protections contemplated in the NOI.[11]

Through its compliance monitoring and enforcement program and other tools, NERC will continue evaluating the manner in which entities implement the controls required in the CIP Reliability Standards and the effectiveness of those controls in securing the BPS. Observing the manner in which entities isolate certain critical BES Cyber Systems (e.g., SCADA/EMS) from the Internet or use application whitelisting in an operational environment, is essential to understanding whether additional protections are needed and the manner in which those protections should be applied without undue interference with operational needs. As it does with all of its standards, if NERC identifies an area requiring additional enhancement, it will address the issue through a combination of standards development activity and its other reliability tools, including security guidelines, training exercises, and alerts.

Further, pursuant to Order No. 822, NERC is required to conduct a comprehensive study, and submit a report by July 2017, on the strength of the remote access controls in the CIP Reliability Standards, the risks posed by remote access-related threats and vulnerabilities, and

---

[9] NOI at PP 1, 9, 13.

[10] *Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,137 (2016).

[11] Applicable Requirements for low impact BES Cyber Systems do not begin to become effective until April 1, 2017.

appropriate mitigating controls.[12] As entities often use Internet connections for remote access, assessing the need for and the reliability impact of mandating separation between the Internet and BES Cyber Systems in Control Centers performing transmission operator functions cannot be accomplished without addressing remote access issues. Similarly, application whitelisting could have implications for remote access capabilities for vendors, as discussed above. Given the relationship between the additional protections contemplated in the NOI and remote access, the results of NERC' study must inform any analysis of the need for and impact of those additional protections.

Moreover, pursuant to Order Nos. 822 and 829, NERC is currently developing modifications to its CIP Reliability Standards to address certain issues connected with the issues addressed in the NOI. Specifically, under Order No. 822, the Commission directed NERC to modify the CIP Reliability Standards to include additional protections for communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers. Including such protections would enhance security and help mitigate the risks of Internet borne threats. Any proposed protections in response to the Order No. 822 directive should be considered when evaluating whether to mandate separation between the Internet and BES Cyber Systems in Control Centers performing transmission operations.

In Order No. 829, the Commission directed NERC to develop modifications to the CIP Reliability Standards to address supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The Commission stated that the new or modified Reliability Standard should address

[12] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037 at PP 3, 18, 64 (2016).

the following security objectives: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. In addressing these objectives, additional protections designed to mitigate the risks associated with Internet connectivity and malicious cyber activity will be included in the CIP Reliability Standards. As such, any modifications to the CIP Reliability Standards in response to Order No. 829 must inform an evaluation as to the need for and implications of requiring Internet isolation and application whitelisting, as contemplated in the NOI.

For the reasons stated above, NERC's evaluation of (1) the manner in which Responsible Entities implement the existing CIP Reliability Standards, (2) the sufficiency of the existing remote access protections, and (3) the directives of Order Nos. 822 and 829, must inform the Commission's inquiry regarding Internet isolation and application whitelisting. Any attempt to answer the Commission's questions in the NOI would be deficient without the benefit of this additional information.

Any additional directives at this time would also increase an already significant workload for NERC and industry with respect to implementation of and development of modifications to the CIP Reliability Standards. Significant industry resources are devoted to implementing the CIP Reliability Standards approved in Order Nos. 791 and 822. Entities are still in the early stages of implementing the Requirements applicable to high and medium impact BES Cyber Systems, which became effective on July 1, 2016. In addition, entities must also devote resources to implementing the Requirements applicable to low impact BES Cyber Systems, which become effective beginning on April 1, 2017. As low impact BES Cyber Systems represent the majority of BES Cyber Systems on the Bulk Electric System and have never been subject to the CIP Reliability

Standards, NERC expects that entities must devote significant resources to those implementation activities.

Further, as mentioned above, NERC and its stakeholders are also currently working on a number modifications to the CIP Reliability Standards to address outstanding Commission directives and other issues that NERC and stakeholders identified during implementation activities. Specifically, as outlined in the Standards Authorization Request ("SAR") for NERC Project 2016-02 – Modification of CIP Standards, in addition to the directive related to communication links and sensitive data exchanged between Control centers, NERC is currently developing the following modifications to address directives from Order No. 822:[13]

- Modifications to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems.
- Modification to the definition "Low Impact External Routable Connectivity" to be consistent with the commentary in the Guidelines and Technical Basis section of Reliability Standard CIP-003-6.

As further outlined in the SAR, the standard drafting team ("SDT") for Project 2016-02 is also evaluating the following issues identified during implementation activities to determine whether additional modifications are necessary:

- The scope of the definitions of "Cyber Asset" and "BES Cyber Asset."
- The clarity of the requirements applicable to network and externally accessible devices.
- The impact designation for BES Cyber Systems associated with Control Centers Performing the functional obligations of a Transmission Operator (TOP).
- The application of the CIP Reliability Standards to the use of virtualization technologies.
- The scope of and requirements related to CIP Exceptional Circumstances.

[13] The SAR us available at: http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/CIP_SAR_822_directives_V5TAG_2016June1_clean.pdf.

Additionally, as noted above, pursuant to Order No. 829, the Commission has directed NERC to develop modifications to the CIP Reliability Standards to address supply chain risk management. The modifications are due within a year of the effective date of Order No. 829. NERC expects this project to require significant ERO and stakeholder resources.

II. CONCLUSION

As discussed herein, the additional protections discussed in the NOI offer potential security benefits. The impact of those protections on operations, however, must be further evaluated to understand when and how those protections could be implemented without undue interference with the needs of Responsible Entities and reliable operations. For the reasons discussed herein, NERC respectfully requests that that the Commission not direct modifications to the CIP Reliability Standards at this time to provide NERC additional time to more comprehensively evaluate the need for and potential drawbacks to mandating Internet isolation and application whitelisting.

Respectfully submitted,

/s/ Shamai Elstein
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

Date: September 26, 2016