UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee and Petition to Order Mandatory Reliability Standards for Equipment and Monitoring Systems Marketed from the People's Republic of China	**)** **)** **)** **)** **)** **)**	**Docket No. EL21-99-000**

MOTION TO INTERVENE AND COMMENT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

September 15, 2021

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee and Petition to Order Mandatory Reliability Standards for Equipment and Monitoring Systems Marketed from the People's Republic of China	**)** **)** **)** **)** **)** **)**	**Docket No. EL21-99-000**

MOTION TO INTERVENE AND COMMENT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pursuant to Rules 206, 212, and 214 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Rules of Practice and Procedure[1] and the Commission's Notice of Complaint,[2] the North American Electric Reliability Corporation ("NERC") moves to intervene and comment on the Complaint filed by Michael Mabee ("Complainant") on August 26, 2021 in the above-captioned docket ("Complaint").

The Complaint claims that (i) entities in the Bulk-Power System ("BPS") are buying and installing critical equipment from the People's Republic of China; (ii) there is no requirement that existing Chinese equipment be checked for risks and vulnerabilities; and (iii) there is no requirement that newly imported Chinese equipment be checked for risks and vulnerabilities.[3] The Complaint requests the Commission: (i) issue a public notice of the Complaint; (ii) investigate the Complaint; (iii) direct NERC to conduct survey of all registered entities in the BPS to determine what Chinese equipment is in use; (iv) direct NERC to submit a proposed Reliability Standard for

1 18 C.F.R. §§ 385.206, 385.212, and 385.214 (2020).
2 Notice of Complaint, Docket No. EL21-99-000 (August 31, 2021).
3 Complaint at 1.

testing and security of Chinese equipment; and (v) work with state public utility commissions to encourage adoption of the Reliability Standard for protection of portions of the grid under state jurisdiction.[4]

NERC takes seriously its role in supporting entities to identify threats and maintain a reliable, secure, and resilient BPS. As such, NERC is well aware of the threat identified by the Department of Energy that "the government of the People's Republic of China is equipped and actively planning to undermine the electric power system in the United States."[5] NERC agrees with the Complainant that industry should take the necessary steps to ensure that the BPS is secure against any adversarial nation-states attempting to exploit vulnerabilities. However, NERC disagrees with the Complainant's proposed course of action to address such threats and notes that the Complainant is incorrect in stating that there are no NERC Reliability Standards that address this risk. Furthermore, the Complaint fails to meet the minimum requirements for filing a complaint, and a complaint proceeding could potentially duplicate or even hamper current efforts to address the threat. As discussed below, NERC moves to intervene and comment in response to the Complainant's assertions and recommendations and requests that the Commission deny the Complaint.

[4] *Id.* at 1 and 13.

[5] Department of Energy, *Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure*, 86 Fed. Reg. 21,309, 21,310 (Apr. 22, 2021).

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[6]

Lauren Perotti*
Senior Counsel
Marisa Hecht*
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
marisa.hecht@nerc.net

II. MOTION TO INTERVENE

NERC has a substantial interest in this proceeding as the Complainant seeks to have the Commission direct NERC to develop a Reliability Standard.[7] By enacting the Energy Policy Act of 2005,[8] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the BPS, and with the duties of certifying an Electric Reliability Organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. The Commission certified NERC as the ERO in 2006.[9]

As the ERO, NERC's mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.[10] Under its FERC-approved Rules of Procedure, NERC

---

6 Persons to be included on the Commission's service list are identified by an asterisk.

7 Complaint at 13. NERC notes that the Complainant, as a private citizen, is not subject to the NERC Reliability Standards, including the CIP Reliability Standards.

8 16 U.S.C. § 824o.

9 *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030, *order on compliance*, 118 FERC ¶ 61,190, *order on reh'g*, 119 FERC ¶ 61,046 (2007), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

10 https://www.nerc.com/AboutNERC/Pages/default.aspx.

develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of the NERC Rules of Procedure ("ROP") and the NERC Standard Processes Manual ("SPM").[11] NERC and the Regional Entities are responsible for monitoring, assessing, and enforcing compliance with Reliability Standards in the United States in accordance with Section 400 (Compliance Enforcement) of the ROP and the NERC Compliance Monitoring and Enforcement Program.[12]

No other party can adequately represent NERC's interests or adequately respond to Complainant's allegations on NERC's behalf. Therefore, it is in the public interest to permit this intervention.

III. SUMMARY

A. Summary of the Complaint

The Complainant alleges that: (1) "entities in the U.S. [BPS] as well as the overall U.S. electric grid are buying critical equipment from the People's Republic of China to install into… critical electric infrastructure that the Communist regime's state sponsored, and state supported hackers, are already probing and attacking";[13] (2) "[t]here is no requirement that existing Chinese equipment or systems already installed in the electric grid be checked and tested for risks and vulnerabilities";[14] and (3) "[t]here is no requirement that newly imported Chinese equipment or

[11] The NERC Rules of Procedure are available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

[12] *Id*. The NERC Compliance Monitoring and Enforcement Program is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4C_CMEP_06082018.pdf.

[13] Complaint at 1.

[14] *Id.*

systems be checked and tested for risks and vulnerabilities before being installed on the electric grid."[15] The Complainant requests that the Commission:

i. Issue a public notice of the complaint;

ii. Investigate this complaint;

iii. Direct NERC to conduct a survey of all registered entities in the BPS to determine what Chinese equipment is in use;

iv. Direct NERC to submit a proposed Reliability Standard for testing and security of Chinese equipment; and

v. Work with state public utility commissions to encourage adoption of the Reliability Standard for protection of portions of the grid under state jurisdiction.[16]

B. Summary of NERC's Comments

The Commission should deny the Complaint because it fails to meet the minimum requirements applicable to complaints under the Commission's Rules of Practice and Procedure,[17] incorrectly characterizes the current body of Reliability Standards as it relates to the reliability threat identified in the Complaint, and seeks relief that is not only duplicative of current efforts to address the threat, but could hamper those efforts.

Under Rule 203 of the Commission's Rules of Practice and Procedure, pleadings must set forth the basis in fact and law for the positions taken.[18] Rule 206 provides eleven elements that a complaint must contain, including the following, among others: (a) clearly identify the alleged action or inaction claimed to violate applicable statutory or regulatory requirements, (b) set forth the business, commercial, economic, or other issues presented by the action or inaction "as such relate to or affect the complainant," (c) indicate the practical, operational, or other nonfinancial

---

15 *Id.*

16 Complaint at 1 and 13.

17 *See* 18 C.F.R. § 385.206.

18 18 C.F.R. § 385.203(a)(7).

impacts imposed as a result of the action or inaction, including, where applicable, the environmental, safety, or reliability impacts of the action or inaction; and (d) make a good faith effort to quantify the financial impact or burden created for the complainant due to the action or inaction.[19] Long-standing Commission precedent provides that "rather than bald allegations, [a complainant] must make an adequate proffer of evidence including pertinent information and analysis to support its claims."[20]

The Complainant failed to provide a basis for a Complaint and failed to demonstrate the existence of any action or inaction that is inconsistent with applicable statutory and regulatory law or any other alleged wrong over which the Commission may have jurisdiction. The Complaint reflects the Complainant's misunderstanding of the application of NERC Reliability Standards and incorrectly states that there are no requirements to assess new or existing equipment for risks and vulnerabilities. As discussed further below, Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 include requirements that address the risk of equipment that is vulnerable to or compromised by adversarial nation-states. NERC continues to assess the efficacy of these Reliability Standards at the direction of the NERC Board of Trustees. For example, NERC is currently revising Reliability Standard CIP-003-8 to expand supply chain requirements to assets containing low impact Bulk Electric System ("BES") Cyber Systems.

---

[19] 18 C.F.R. § 385.206(b) (listing the full list of elements for a complaint) (NERC does not waive objection to the Complaint's failure to meet other elements of a properly pleaded complaint but is simply highlighting these elements); *Complaint of Michael Mabee Related to Reliability Standards*, Order Denying Complaint, 175 FERC ¶ 61,163, at P 14 (2021).

[20] *Ill. Mun. Elec. Agency v. Cent. Ill. Pub. Serv. Co.*, Order Dismissing Complaint Without Prejudice, 76 FERC ¶ 61,084 at 4 (1996); *CAlifornians for Renewable Energy, Inc., (CARE) and Barbara Durkin v. Nat'l Grid, Cape Wind, and the Mass. Dep't of Pub. Util.*, Order Dismissing Complaint, 137 FERC ¶ 61,113, at PP 2, 31-32 (2011); *CAlifornians for Renewable Energy, Inc., Michael E. Boyd, and Robert M. Sarvey v. Pac. Gas and Elec. Co.*, Order Dismissing Complaint, 143 FERC ¶ 61,005 at P 2 (2013); and *Citizens Energy Task Force and Save Our Unique Lands v. Midwest Reliability Org., et al*., Order Dismissing Complaint, 144 FERC ¶ 61,006, at P 38 (2013).

Moreover, NERC also takes a defense-in-depth approach by engaging in activities in addition to mandatory Reliability Standards to help industry mitigate supply chain risks, in particular those posed by adversarial nation-states. These efforts include alerts to industry on emerging supply chain risks, an initiative dedicated to supply chain risk mitigation, discussions at grid security exercises, and collaboration with industry stakeholders. These activities complement the Reliability Standards by providing timely and specific information and recommendations to address newly identified and evolving threats posed by adversarial nation-states.

For these reasons, the Commission should decline to provide the relief requested by the Complainant. The Commission should not engage in a complaint proceeding at this time as it would be duplicative and potentially hamper the efforts already underway.

IV. COMMENTS

A. The Complaint should be denied because the Complaint fails to meet the minimum requirements of the FPA and the Commission's regulations.

The Complaint asserts that (i) entities in the BPS are buying and installing critical equipment from the People's Republic of China; (ii) there is no requirement that existing Chinese equipment be checked for risks and vulnerabilities; and (iii) there is no requirement that newly imported Chinese equipment be checked for risks and vulnerabilities.[21] The Complaint has failed to meet its burden under the Commission's rules. The Complainant does not provide proof or specific examples as to how these actions or inactions allegedly violate applicable law or regulations. The Complainant's sole basis of the Complaint rests on an inaccurate understanding of the NERC Reliability Standards. As described below, the supply chain requirements within Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 require Responsible Entities to assess

[21] Complaint at 1.

risks to the BES from vendor products and services during procurement of applicable BES Cyber Systems. In addition, CIP-010-3 requires Responsible Entities to perform vulnerability assessments of existing applicable BES Cyber Systems. Because the Complainant has failed to support its assertions, as required by the Commission's rules and regulations, the Complaint should be denied.

Reliability Standard CIP-013-1 requires Responsible Entities[22] to develop and implement plans to address supply chain cybersecurity risks. One such risk Responsible Entities must consider during the planning and procurement of high and medium impact BES Cyber Systems is the risk posed by adversarial nation-states compromising equipment. As stated in the petition for approval of CIP-013-1, the security objective of the supply chain cybersecurity risk management plans is to ensure that Responsible Entities consider the security, integrity, quality, and resilience of the supply chain and take appropriate mitigating action when procuring BES Cyber Systems to address threats and vulnerabilities in the supply chain.[23]

The supply chain cybersecurity risk management plans that entities must adopt include processes to: (1) identify and assess cybersecurity risks to the BES from vendor products and services; and (2) include specified security concepts in their procurement activities for high and medium impact BES Cyber Systems, including (i) vendor security event notification processes, (ii) coordinated incident response activities, (iii) vendor personnel termination notification for

[22] As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entities subject to the CIP Reliability Standards.

[23] *Petition of NERC for Approval of Proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management*, Docket No. RM17-13-000, at 13 (Sep. 26, 2017).

employees with access to remote and onsite systems, (iv) vulnerability disclosures, (v) software integrity and authenticity, and (vi) coordination of controls for vendor remote access.[24]

Additionally, supply chain requirements in CIP-005-6 and CIP-010-3 address specific risks related to vendor remote access and software integrity and authenticity, respectively, in the operational phase of the system life cycle.[25] Pursuant to Requirement R2, Parts 2.4 and 2.5 of Reliability Standard CIP-005-6, Responsible Entities must have one or more methods for: (1) determining active vendor remote access sessions (Part 2.4); and (2) disabling active vendor remote access (Part 2.5).[26] The security objective of these requirement parts is to control vendor remote access to mitigate risks associated with unauthorized access.[27]

As described above, the CIP Reliability Standards speak to supply chain risks generally, but that is by design as these risks continue to evolve. For instance, NERC expects Responsible Entities to assess the risks posed by adversarial nation-states when planning for procurement of high and medium impact BES Cyber Systems as part of their CIP-013-1 processes. Pinpointing a specific nation-state within the requirements, as proposed by the Complainant, would prevent the applicability of the requirements to other nation-states that may pose a threat to the supply chain.

Furthermore, Reliability Standard CIP-010-3, Requirement R3 addresses vulnerabilities on existing BES Cyber Systems. Vulnerability assessments can include identifying active devices and communication paths, as well as open ports and services, to ensure that the network architecture matches the documented architecture.

---

24 *Id.* 13-14.
25 *Id.*
26 *Id.*
27 *Id.*

As the Complaint rests on a misunderstanding of the NERC Reliability Standards and fails to demonstrate the claimed actions or inactions have allegedly violated any applicable law or regulation, the Commission should deny the Complaint.

B. The Complaint should be denied because the relief sought is unsupported and premature given current activities.

NERC notes that Reliability Standards are just one tool NERC uses to support mitigation of supply chain risks and to help to ensure the reliability and security of the BPS. As noted in NERC's 2021 State of Reliability Report, a combination of activities supporting a defense-in-depth approach to supply chain risk mitigation has helped avoid cyber or physical security incidents on BES facilities that resulted in a loss of load, but the State of Reliability Report also underscores the vigilance NERC and industry will exercise going forward.[28]

While mandatory Reliability Standards play an integral role in securing the BPS, NERC is committed to using all available approaches to support supply chain risk mitigation, especially those approaches that can be quickly deployed to address this ever-evolving threat. NERC is currently engaged in the following initiatives to help industry address supply chain risks and support the goal of avoiding cyber or physical security incidents on BES facilities that impact BPS reliability:

- Supply Chain Risk Mitigation Program: In 2017, NERC initiated the Supply Chain Risk Mitigation Program, a collaborative program with industry, trade organizations, and key stakeholders to support implementation of the supply chain standards and manage the effective mitigation of supply chain risks.[29] Since its inception, the program has produced several studies, data requests, reports, guidelines, and webinars, among other activities, that focus on reducing the risk posed by supply chain compromise, including those risks posed by adversarial nation-states. Furthermore, the NERC Board has directed that NERC's Supply Chain Risk

[28] NERC 2021 State of Reliability Report at 72, https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2021.pdf.

[29] The website for the Supply Chain Risk Mitigation Program is available at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

Mitigation Program include the following efforts to enhance reliability through mitigation of supply chain risks:

1. Perform cyber security supply chain risk study, including an independent assessment of supply chain risks;
2. Communicate supply chain risks to industry;
3. Request forums and trade associations to develop white papers addressing best and leading practices for supply chain management; and
4. Evaluate the effectiveness of the supply chain standards.

- NERC Alerts:[30] NERC has issued several supply chain alerts and advisories within the past few years, many of which discussed risks associated with non-U.S. vendors. These tools provide entities with information and, in the case of the Level 2 Alerts, recommended actions to address these risks. FERC reviews these alerts before they are sent to industry and are updated consistent with NERC Rules of Procedure section 810. These alerts have made recommendations and gathered the extent of conditions on numerous supply chain risks, addressing many threat actors. In order to assure the security of the BPS, some of these alerts are nonpublic, while others are public.
- E-ISAC All-Points Bulletins: Throughout 2021, the E-ISAC issued a number of All-Points Bulletins related to adversary compromises of software supply chain tools, such as on-premise Microsoft Exchange servers, Ivanti's Pulse Connect Secure products, Kaseya remote management tools, and the Blackberry QNX vulnerability in real-time operating systems.
- Whitepapers:
    - NERC and FERC staff developed a joint whitepaper on Network Interface Controllers.[31] The whitepaper outlines a noninvasive technique to help the electric sector identify vendors of components, including those supported by the People's Republic of China, on their networks so that they can take any necessary action to mitigate potential risks to the BPS.
    - NERC and FERC staff published a joint whitepaper on the SolarWinds event and related supply chain compromise.[32]

---

[30] As defined in NERC Rules of Procedure Section 810, NERC Alerts are divided into three distinct levels, as follows: (1) Industry Advisory: Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary; (2) Recommendation to Industry: Recommends specific action be taken by registered entities. A response from recipients, as defined in the alert, is required; and (3) Essential Action: Identifies actions deemed to be "essential" to BPS reliability and requires NERC Board of Trustees' approval prior to issuance. Like recommendations, essential actions also require recipients to respond as defined in the alert. The NERC Rules of Procedure are available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20190125.pdf.

[31] FERC and NERC, *Joint Staff White Paper on Supply Chain Vendor Identification - Noninvasive Network Interface Controller* (July 31, 2020), https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf.

[32] FERC and NERC, *SolarWinds and Related Supply Chain Compromise TLP:WHITE - Lessons for the North American Electricity Industry* (July 2021),

- Data Requests, Assessments, and Reports:
  - NERC analyzes supply chain risk through assessments and other reports, such as the Special Report: Pandemic Preparedness and Operational Assessment: Spring 2020 and State of Reliability Reports.[33]
  - To better understand supply chain risks, NERC collected data from registered entities pursuant to a request for data or information under Section 1600 of the NERC Rules of Procedure.[34] NERC analyzed the data received to understand the implications of supply chain vulnerabilities not covered in CIP-013-1, CIP-005-6, and CIP-010-3, producing a final report.[35]
- GridEx: E-ISAC included a supply chain topic in NERC's Grid Security Exercises GridEx IV and V and is planning to do so again in GridEx VI in November 2021.
- NERC Reliability and Security Technical Committee ("RSTC"): In 2019, the RSTC's Supply Chain Working Group developed 14 guidelines regarding supply chain security and a widely distributed "letter to industry" with information for industry suppliers. In 2020, two more guidelines were developed as well as a webinar series that featured discussions about each guideline.

As demonstrated by the extensive list of activities above, NERC employs a comprehensive approach to accomplish its mission of maintaining a reliable BPS in the face of supply chain threats, including those posed by adversarial nation-states. The Complainant has failed to demonstrate that these activities, in addition to the current Reliability Standards, are deficient in addressing the risk of compromised equipment to the reliability of the BPS. As such, the requested relief sought of developing Reliability Standards is unsupported.

---

https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds%20and%20Related%20Supply%20Chain%20Compromise%20White%20Paper.pdf.

[33] NERC, *Special Report, Pandemic Preparedness and Operational Assessment* (Spring 2020), Special Report: Pandemic Preparedness and Operational Assessment: Spring 2020; State of Reliability Reports are available at https://www.nerc.com/pa/RAPA/PA/Pages/default.aspx.

[34] NERC, *Request for Data or Information: Supply Chain Risk Assessment Data Request* (Aug. 2019): https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Final%201600%20data%20request%20-%20clean.pdf.

[35] NERC, *Supply Chain Risk Assessment: Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request* (Dec. 2019), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf. NERC recommended revising CIP-013-1 in this report, although ultimately the Board resolved to revise CIP-003-8.

In addition to NERC activities, there is a comprehensive plan put forth by the Biden Administration to assess and mitigate supply chain risks. Effective April 20, 2021, the Biden Administration revoked Executive Order 13290, imposing a ban on acquisition of certain equipment from foreign adversaries, to "create a stable policy environment."[36] On that same date, the Department of Energy, in coordination with the electric industry and the Cybersecurity and Infrastructure Security Agency, launched an initiative known as the "100 day plan" that focuses on actions to address cybersecurity threats from adversaries targeting electric utilities' industrial control systems.[37] As part of this initiative, the Department of Energy issued a new Request for Information ("RFI") focusing on preventing exploitation and attacks by foreign threats to the United States supply chain, including that of the nation's critical infrastructure. In issuing this RFI, the Department of Energy recognized the "growing prevalence of essential electric system equipment being sourced from China presents a significant threat to U.S. critical infrastructure."[38] Public comments on this RFI closed on June 7, 2021, and the Department of Energy is considering next steps based on comments received. Any action by FERC should take into account the impacts of any recommended next steps from this RFI. As such, given this pending action, granting the relief requested by the Complainant is premature.

---

[36] Executive Order 13990 of January 20, 2021, *Protecting Public Health and the Environment and Restoring Science To Tackle the Climate Crisis*, 86 Fed. Reg. 7,037 (Jan. 25, 2021).

[37] Department of Energy, News Release, *DOE Kicks off 100-Day Plan to Address Cybersecurity Risks to the U.S. Electric System, Seeks Input from Stakeholders on Safeguarding U.S. Critical Energy Infrastructure* (Apr. 20, 2021), https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0.

[38] Department of Energy, RFI Frequently Asked Questions, https://www.energy.gov/oe/securing-critical-electric-infrastructure.

V. CONCLUSION

WHEREFORE, for the reasons stated above, NERC respectfully requests that the Commission grant this motion to intervene, accept the comments herein, and deny the Complaint.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: September 15, 2021

CERTIFICATE OF SERVICE

I hereby certify that I have this day served a copy of this document upon all parties listed on the official service list compiled by the Secretary in the above-captioned proceeding, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated at Washington, D.C., this 15th day of September, 2021.

/s/ Marisa Hecht
Marisa Hecht
Counsel for the North American Electric Reliability Corporation