UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. RD22-3**

REPLY COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The North American Electric Reliability Corporation ("NERC") submits the following reply comments in response to the Edison Electric Institute's ("EEI") March 15, 2022 motion to intervene and comments in the above captioned docket.[1] EEI opposes NERC's proposal to modify the compliance section of Reliability Standard CIP-014-2 ("CIP-014") to remove the provision, unique to CIP-014, that provides for all evidence demonstrating compliance with the standard to be retained at the transmission owner's or operator's facility. EEI posits that the provision is necessary to ensure the security of CIP-014. This position is not correct. As discussed in NERC's petition and reiterated below, the proposed modification would not decrease the protection of any highly sensitive compliance evidence nor does it favor ease of access over the safety, security, and reliability of the electric grid, as EEI claims. The proposed modification is necessary to ensure that NERC and the Regional Entities (collectively, the "ERO Enterprise") may monitor compliance with the standard effectively. Inability to monitor compliance could ultimately reduce the overall physical security of the facilities subject to CIP-014.

As discussed in NERC's petition, there is no continued justification for the provision in the compliance section of CIP-014 that requires all evidence demonstrating compliance with the standard to be retained at the Transmission Owner's or Transmission Operator's facility. EEI's

[1] NERC seeks leave to submit this reply and requests that the Commission waive Rule 213(a)(2), 18 C.F.R. 385.213(a)(2), for this purpose. This reply should be permitted because it enhances the record by clarifying and completing the record on issues raised by EEI.

assertion that retaining the provision is the only way to ensure the protection of CIP-014 evidence is incorrect. While NERC agrees with EEI on the importance of protecting the confidentiality of the highly sensitive information used to demonstrate compliance with CIP-014, with the use of the ERO Secure Evidence Locker ("SEL"), NERC has a highly secure means of collecting and analyzing CIP-014 evidence in the same manner as any other sensitive evidence collected as part of Compliance Monitoring and Enforcement Program ("CMEP") activities.

As detailed in the petition, the ERO Enterprise developed the ERO SEL for temporary storage of all Registered Entity artifacts (i.e., compliance evidence). The ERO SEL is a highly secure, isolated, and on-premises at NERC environment designed to protect submitted Registered Entity artifacts. The ERO SEL enables a Registered Entity to securely submit evidence through an encrypted session. The artifacts are encrypted immediately upon submission, securely isolated per Registered Entity, never extracted, never backed up, and subject to proactive and disciplined destruction policies. The ERO SEL architecture and operational model adhere to the National Institute of Standards and Technology 800-171 security control framework, which is established to protect Controlled Unclassified Information ("CUI") in nonfederal systems (Critical Energy Infrastructure Information is classified as CUI).[2] The ERO SEL is thus designed to significantly reduce risk of evidence loss and exposure.

EEI's concern regarding the ERO SEL functioning as a central repository for CIP-014 evidence is overstated given the security architecture and protections mentioned above. It is important to recognize that there will be limited CIP-014 evidence aggregated in the SEL at any given time because: (1) artifacts included in the ERO SEL are encrypted, never backed-up, and

[2] National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171, rev. 2 (Feb. 2020), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

removed after the CMEP engagement has concluded; and (2) there are only a limited set of CIP-014 engagements at any one time.

Additionally, as further discussed in NERC's petition, should an entity have any lingering concerns about submitting CIP-014 or other compliance evidence to the SEL, it has two reasonable alternatives. First, the ERO also has an alternative framework (or exception process) that allows for a Registered Entity to collaborate with its Compliance Enforcement Authority ("CEA") on effective and secure evidence submittal outside of the ERO SEL. This alternative, for instance, could include an onsite-only review of any highly sensitive information or a review of evidence through a secure videoconferencing platform.

Second, even if the Registered Entity and its CEA cannot agree on an alternative framework for reviewing compliance evidence, a Registered Entity may choose to develop its own SEL rather than use the ERO SEL. By using its own SEL, an entity could address EEI's concerns about unauthorized access to its CIP-014 evidence.

EEI characterizes NERC's proposal as allowing "ease of access" to "take precedence over the safety, security and reliability of the electric grid." This characterization is misleading. NERC is not seeking the proposed modification to provide the ERO Enterprise a greater "ease of access"; it is to ensure that they have the ability to monitor compliance effectively and, in some cases, at all. Over the last two years, there have been instances in which Registered Entities, citing their pandemic-related restrictions, refused to allow Regional Entities to come on site to monitor compliance. While such a prohibition may have been appropriate at that time, certain entities also refused to allow a review of evidence using a secure videoconferencing platform. The end result was increased risk, in certain instances, because the ERO Enterprise had no mechanism with which to monitor compliance with CIP-014 until the entity, at its own discretion, lifted its pandemic-

related restriction. In contrast, NERC was able to effectively and securely monitor other Reliability Standards remotely, including other sensitive CIP-related requirements, as no other NERC reliability standard contains the on-site evidence provision as in CIP-014.

EEI states that "such concerns are diminishing as the country begins to exit the pandemic". There is no certainty, however, that the country is in fact exiting the pandemic over the long term. As has occurred previously, when infection rates are low, as is currently the case for most areas of the U.S. in March 2022, pandemic-related restrictions are decreased or removed all together. When infection rates begin to climb, however, those same restrictions are often put back in place. There is no guarantee infections will remain low or that the pandemic related-restrictions will not return. There is also no guarantee that going forward there will not be another set of circumstances, pandemic-related or otherwise, that limits the ERO Enterprise's ability to review evidence on site.

It is imperative, therefore, that the provision in the CIP-014 compliance section be removed so that the ERO Enterprise has the ability to monitor compliance with CIP-014 and help ensure that key infrastructure is adequately protected. As discussed above, removing the provision addresses an ongoing risk of not being able to monitor CIP-014 effectively. It is not a trade-off between security and access. Between the ERO SEL and the alternatives discussed above, the ERO Enterprise has mechanisms to review CIP-014 evidence securely without the provision in the compliance section. Pursuant to the Federal Power Act, Commission regulations, and the NERC Rules of Procedure ("ROP"), the ERO Enterprise has the authority to collect evidence in a manner it deems most appropriate from a Registered Entity to carry out the CMEP.[3] NERC respectfully

[3] The NERC ROP, Appendix 4C, Section 3.0, states: "The Compliance Enforcement Authority has authority to collect Documents, data and information in the manner it deems most appropriate, including requesting copies of Documents, data and information to be made and removing those copies from the Registered Entity's location in accordance with appropriate security procedures conforming to Section 1500 of the Rules of Procedure and other safeguards as appropriate in the circumstances to maintain the confidential or other protected status of the

requests that the Commission approve removal of the provision, to the extent such approval is necessary, as soon as practicable.

Respectfully submitted,

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

Counsel for the North American Electric Reliability Corporation

Date: March 21, 2022

Documents, data and information, such as information held by a governmental entity that is subject to an exemption from disclosure under the United States Freedom of Information Act, or a comparable state or provincial law, that would be lost of [sic] the information were placed into the public domain." NERC Rules of Procedure, Appendix 4C, available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.