NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

April 23, 2019

VIA ELECTRONIC SUBMISSION

Mr. Leonard M. Tao
Director
Office of External Affairs
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Submitter's Rights Letter, FOIA-2019-19

Dear Mr. Tao:

In response to your letter, dated April 16, 2019, regarding a Freedom of Information Act ("FOIA") request to obtain the NERC Full Notice of Penalty in various dockets,[1] the North American Electric Reliability Corporation ("NERC") maintains that the information requested should not be released because it is exempt from disclosure under FOIA. As FERC has previously recognized, NERC Full Notices of Penalty are exempt from public disclosure under FOIA Exemptions 3 and 7(F) as they contain Critical Energy/Electricity Infrastructure Information ("CEII") or information that would otherwise pose a risk to the security of a NERC registered entity.[2]

NERC filed its CIP Notices of Penalty in the dockets subject to this request on a nonpublic basis under Section 39.7(b)(4) of the Commission's regulations because they contained information that would jeopardize the security of the BPS if publicly disclosed.[3] The nonpublic version of the Notices of Penalty included the identity of the registered entities, information that could lead to the identity of the registered entities, and information about the security of the registered entities' systems and operations, such as specific configurations or tools the registered entities use to manage their cyber systems. The public version of the Notices of Penalty did not include the identity of the registered entities but did include

[1] The requestor is seeking information regarding numerous docket numbers. However, given the volume of information requested, your letter noted that FERC staff is processing the request on a rolling basis, with the following six docket numbers addressed first: NP14-42-000; NP14-45-000; NP14-46-000; NP14-48-000; NP15-5-000; NP15-6-000; NP15-9-000; NP15-10-000; and NP15-11-000.

[2] *See* Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018). To date, the Commission has directed public disclosure regarding the disposition of CIP violations in only a small number of cases. *See* id. and previous decisions in this FOIA docket, wherein the Commission has disclosed the name of the registered entity in three cases while continuing to treat the remaining information in the Notices of Penalty as nonpublic.

[3] Section 39.7(b)(4) of the Commission's regulations states: "The disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise."

anonymized information about the registered entities' systems and operations, with varying levels of detail. As the Commission has previously recognized, information related to CIP violations and cyber security issues, including the identity of the registered entity, may jeopardize BPS security because "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize system security, allowing persons seeking to do harm to focus on a particular entity in the Bulk-Power System."[4]

Consistent with the Commission's statement and Section 39.7(b)(4), NERC treated as nonpublic the identity of the registered entities and any information that could lead to the identification of the registered entities. Entities providing electricity to the people of the United States are subject to constant attacks by malicious parties, including some supported by foreign governments.[5] Identifying the registered entities in these cases would have highlighted entities whose implementation of the CIP standards was less than adequate and may have been more vulnerable to cyber attacks, which in most cases posed a serious risk to the BPS. Consistent with the purpose of Section 39.7(b)(4), NERC has taken care to ensure that Notices of Penalty do not become mechanisms for adversaries to identify more vulnerable targets and jeopardize the security of the BPS.

The Commission's expectation that NERC should not identify entities violating CIP Reliability Standards was longstanding[6] and most recently reflected in FERC's 2014 *Order on the Electric Reliability Organization's Five-Year Performance Assessment*. In that order, the Commission stated that, "[w]ith respect to concerns and questions raised regarding NERC's protection of information deemed to be confidential, particularly as related to cybersecurity incidents or CIP violations, we believe that NERC currently has adequate rules and procedures in place to protect against improper disclosure of sensitive information (…)."[7]

---

[4] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, Order No. 672, 2006-2007 FERC Stats. & Regs., Regs. Preambles ¶ 31,204 at P 538 (*Order No. 672)*.

[5] Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," *Wall Street Journal* (January 11, 2019)(https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112).

[6] *See North American Electric Reliability Corp.*, Order Accepting With Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing, 138 FERC ¶ 61,193 at P 69 (wherein the Commission cited NERC's practice under Section 39.7(b)(4) of not publicly disclosing the entities that violated the CIP Standards). *See also North American Electric Reliability Corp.*, Order on Compliance Filing, 143 FERC ¶ 61,253 at P 37 n.50 (2013)(wherein the Commission emphasizes protecting nonpublic and confidential information and redacting any details that could be used to identify the registered entity for violations of CIP Reliability Standards).

[7] *North American Electric Reliability Corp.*, Order on the Electric Reliability Organization's Five-Year Performance Assessment, 149 FERC ¶ 61,141, at n. 55, P 47, and n. 65 (2014) (in response to a commenter referencing a prior inadvertent disclosure of the identity of an Unidentified Registered Entity sanctioned for violations of CIP Reliability Standards).

NERC also treated as nonpublic any information about the security of the registered entities' systems and operations. Details about an entity's systems, including specific configurations or the tools/programs it uses to configure, secure, and manage changes to its BES Cyber Systems, would provide an adversary relevant information that could be used to perpetrate an attack on the entity and similar entities that use the same systems, products, or vendors.[8] As the Commission has stated, "[g]uarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure."[9]

In addition to the provisions of Section 39.7(b)(4), NERC's nonpublic versions of the Notices of Penalty were also designated as CEII under the Commission's regulations. As noted above, beyond just including the names of the entities and information that could be used to identify the entities, the nonpublic Notices of Penalty included specific vulnerability and design information that could be useful to a person planning an attack on critical infrastructure. For example, the nonpublic Notices of Penalty include the identification of specific cyber security issues, as well as details concerning the types and configurations of the entities' systems and assets. The information also describes strategies, techniques, and solutions to resolve specific cyber security issues. In many cases, the entities may still use the same systems and the same or similar techniques or procedures for security. Also, in some cases, the public Notices of Penalty include information that, when associated with the identity of the registered entity, could still pose a risk to security.

For the reasons stated above, the information contained in the Notices of Penalty subject to the letter still warrants continued nonpublic treatment and should not be released under FOIA Exemptions 3 and 7(F). The Notices of Penalty include detailed descriptions of the facts and circumstances of each violation; the disposition document (either a Settlement Agreement or Notice of Confirmed Violation, between the Regional Entity and the registered entity to resolve the violations); and attachments to the disposition document, including the violation discovery documents, Mitigation Plans, and documentation

[8] *See* "America's Electric Grid Has a Vulnerable Back Door" (detailing phishing and other hacking schemes aimed at utility contractors in order to penetrate utility networks).

[9] *Reliability Standards for Physical Security Measures*, "Order Directing Filing of Standards," 146 FERC ¶ 61,166 at P 10 (2014).

of mitigation completion and verification. Accordingly, NERC objects to the FOIA request and respectfully states that granting any part of the FOIA request could jeopardize the security of the Bulk Power System.

Respectfully submitted,

/s/ Edwin G. Kichline
Edwin G. Kichline

Senior Counsel and Director of Enforcement Oversight
North American Electric Reliability Corporation

cc: Ms. Toyia Johnson, FERC