February 20, 2019

VIA E-MAIL

Mr. Leonard M. Tao
Director, External Affairs
888 First Street, NE
Washington, D.C. 20426
Leonard.tao@ferc.gov

Re: Submitter's Rights Letter, FOIA No. FY19-030

Dear Mr. Tao,

On behalf of our members, the American Public Power Association ("APPA"), the Edison Electric Institute ("EEI") and the National Rural Electric Cooperative Association ("NRECA"), (collectively, the "Trade Associations") respectfully submit the following comments in response to your February 8, 2019 Submitter's Rights Letter to Mr. Kichline, Mr. Berardesco, and Ms. Mendonca, regarding a Freedom of Information Act ("FOIA") request made by Mr. Michael Mabee to obtain the NERC Full Notice of Penalty ("Full NOP") in various dockets ("the FOIA Request").[1]

APPA is the national service organization representing the interests of the nation's 2,000 not-for-profit, community-owned electric utilities. Public power utilities account for 15% of all sales of electric energy (kilowatt-hours) to ultimate customers and collectively serve over 49 million people in every state except Hawaii. Approximately 261 public power utilities are registered entities subject to compliance with North American Electric Reliability Corporation ("NERC") mandatory reliability standards.

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than seven million jobs in communities across the United States. In addition to our U.S. members, EEI has more than 65 international electric companies as International Members, and hundreds of industry suppliers and related organizations as Associate Members. EEI's U.S. members include Generator Owners and Operators, Transmission Owners and Operators, Load-Serving Entities, and other entities that are subject to the mandatory Reliability Standards developed by the NERC and enforced by NERC and the Federal Energy Regulatory Commission ("FERC" or "the Commission"). EEI's members are committed to the reliability and security of the bulk-power system.

[1] FOIA No. FY19-030 (Feb. 8, 2019).

NRECA is the national service organization for the nation's member-owned, not-for-profit electric cooperatives. More than 900 rural electric cooperatives are responsible for keeping the lights on for more than 42 million people across 47 states. Because of their critical role in providing affordable, reliable, and universally accessible electric service, electric cooperatives are vital to the economic health of the communities they serve. Cooperatives serve 56% of the nation's land area, 88% of all counties, and 12% of the nation's electric customers, while accounting for approximately 11% of all electric energy sold in the United States. NRECA's member cooperatives include entities that are subject to the NERC mandatory reliability and cybersecurity standards. Accordingly, NRECA members are directly affected by this FOIA request.

The explanation in the FOIA Request appears to request only the names of the Unidentified Registered Entities ("UREs") for the ten dockets, [2] but the actual request seeks public disclosure of the Full NOPs, which are the versions that include the registered entity names. In addition, the requester has also submitted requests for the same information for not only these ten dockets, but from 232 additional dockets covering Critical Infrastructure Protection ("CIP") reliability standards violations over the past ten years.[3]

The Trade Associations object to the release of the information requested by Mr. Mabee because its disclosure is not required by FOIA and—more importantly—because disclosing this information broadly would unnecessarily jeopardize national security by providing sensitive information about the bulk-power system. For these reasons, the Commission should not release the documents requested.

Even with perfect compliance, cyber vulnerabilities would exist, given the constantly evolving threats to cybersecurity. Each requested NOP, when coupled with the name of the URE and other, already-public information, could provide sufficient information to materially assist those entities that are driven to find and exploit such vulnerabilities. While the Trade Associations object to the release of this information generally because of concerns about the safety and reliability of the bulk-power system, should the Commission determine that it is necessary to provide any element of an NOP in response to the FOIA Request, the Commission should provide both NERC and the URE ample time to review this information and provide a detailed assessment of the potential harm that could result from disclosure. This would be appropriate given the very few days that the UREs and NERC have to analyze and respond to the Submitter's Rights Letter and the FOIA request in general, which seeks the disclosure of thousands, if not tens of thousands, of pages of information. In addition, FERC itself should consider carefully how any piece of information, no matter how seemingly innocuous on its own, could be coupled with other information and used by those seeking to attack the reliability of U.S. energy infrastructure.

---

[2] FERC Docket Nos.: NP10-140-000, NP10-139-000, NP10-138-000, NP10-137-000, NP10-136-000, NP10-135-000, NP10-134-000, NP10-131-000, NP10-130-000, and NP10-150-000.

[3] Request under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (Dec. 18, 2018), https://michaelmabee.info/wp-content/uploads/2018/12/FERC-FOIA-Request-2018-12-18-R.pdf; Request under the Freedom of Information Act (FOIA), 5 U.S.C § 552 (Jan. 12, 2018), https://michaelmabee.info/wp-content/uploads/2019/01/FERC-FOIA-Request-Mabee-2019-01-12-R.pdf.

Release of the requested information by the Commission is not required by FOIA.

The release of the information requested in the December 18, 2018 FOIA request, as amended January 4, 2019, is not required by FOIA or under the Commission's FOIA regulations. The requested information is exempt from disclosure pursuant to 5 U.S.C. 552(b)(3) ("Exemption 3") and 5 U.S.C. 552(b)(7)(F) ("Exemption 7(F)"). Exemption 3 precludes disclosure of information that is prohibited from disclosure by another federal law and Exemption 7(F) precludes the disclosure of "records or information compiled for law enforcement purposes" if the release of such information "could reasonably be expected to endanger the life or physical safety of any individual."[4]

In addition, Section 39.7(b)(4) of the Commission's enforcement of reliability standards regulations provides the exception that "[t]he 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 non-public unless the Commission directs otherwise."[5] The information found within the requested Full NOPs contains details, including the identities of the URE, URE mitigation plans, and other specific security measures taken by particular UREs to address actual security risks identified either in audit or by self-reports. The Commission has consistently protected this information from public disclosure to prevent jeopardizing the security of the bulk-power system. The requested information provides details and strategic security information pertaining to the generation and transmission system that would be useful to a person planning an attack on critical infrastructure. Because this information is protected by FOIA Exemption 3 and it is reasonably foreseeable that disclosure would harm the interests protected by that exemption, this information should not be disclosed by the Commission under Exemption 3.[6]

The Fixing America's Surface Transportation Act, Pub. L. No. 118-94, §61003 (2015); 16 U.S.C. 824o-1(d)(1) ("FAST Act"), specifically exempts Critical Electric Infrastructure Information ("CEII") from disclosure. The FOIA Request seeks copies of documents providing information concerning critical cyber assets and the NERC CIP violations of the UREs treated in the dockets he has identified. This information includes details regarding the physical and cyber safeguards, protections, and vulnerabilities associated with the reliable operation of the bulk-power system, which is CEII. The Commission has a longstanding recognition of the need to protect information associated with critical electric infrastructure as CEII from public disclosure.[7] In addition, FERC has previously responded to a similar request, determining that identification of a URE is protected from disclosure by 5 U.S.C. §§ 552(b)(3) and 7(f).[8] FERC's response letter noted that:

---

[4] 15 U.S.C. §§ 552(b)(3) and 7(F).

[5] Enforcement of Reliability Standards, 18 C.F.R. § 39.7 (b)(4).

[6] 5 U.S.C. § 552(a)(8)(A)(i)(I).

[7] *See, e.g.*, FERC Order 706 (Jan. 18, 2008), at ¶ 330.

[8] FERC Response, FOIA No. FY18-75 (May 25, 2018), https://michaelmabee.info/wp-content/uploads/2018/06/DETERMINATION-LETTER-FOIA-2018-75-R.pdf.

> with respect to the name of the Unidentified Registered entity, disclosing such name could provide a potential bad actor with information that would make a cyber intrusion less difficult. In this regard, public release of the requested documents would provide information which could help breach its network, and allow possible access to non-public, sensitive, and/or confidential information that could be used to plan an attack on energy infrastructure, endangering the lives and safety of citizens.[9]

Accordingly, the release of the information requested is not required by FOIA because Exemption 3 and 7(F) apply, as well as the Commission's regulations on enforcement of the reliability standards. Not only is this information not required to be disclosed pursuant to FOIA Exemption 3, but it is reasonably foreseeable that disclosure would harm the security interests that exemption and the FAST Act explicitly protect.[10]

The Trade Associations oppose the release of the requested documents because the information would be useful to a person planning an attack on the bulk-power system.

The array and capabilities of hostile forces seeking to attack the U.S. electric grid and destabilize the nation has increased in size and sophistication. In the past year, the FBI and United States Department of Homeland Security publicly revealed that a foreign nation-state engaged in a prolonged, "multi-stage intrusion campaign" against U.S. utilities.[11] Also, the United States Department of Justice indicted foreign hackers who successfully penetrated hundreds of U.S. institutions. In releasing the indictment, the Department of Justice specifically called out the grave risk posed by malicious actors targeting the US electric sector, including the Commission itself, for sensitive information.[12]

The FOIA Request to publicize sensitive information about the U.S. electric grid could assist people seeking to attack U.S. electric infrastructure. Even information that some may deem

---

[9] *Id.* at 2. The Trade Associations are aware that the Commission has previously released the name of a URE in response to a similar FOIA request. However, the Commission has not made its decision or reasoning behind it public. As a result, we cannot comment on the applicability of that decision. However, the circumstance is distinguishable based solely on the fact that this request seeks the wholesale release of Full NOPs contained in up to 242 separate dockets. In addition, that one release appears to have been an outlier, and thus has limited (if any) decisional value. For example, the Commission initially denied that request using the same reasoning listed above, and then without explanation reversed that decision. Since the Commission did not explain its reasoning for releasing the information, that decision has limited bearing here. In addition, the Trade Associations understand that two different parties filed FOIA requests for the URE name that was eventually released. We also understand that the Commission released the URE name in response to one FOIA request and withheld it in response to the other. We do not understand why the Commission faced two FOIA requests seeking what we believe to be the same information at approximately the same time, and yet reached two different results, especially since the Commission has not been transparent in its decision-making process.

[10] 5 U.S.C. § 552(a)(8)(A)(i)(I).

[11] United States Computer Emergency Readiness Team (US-CERT), Alert TA18-074A, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (Mar. 16, 2018), https://www.us-cert.gov/ncas/alerts/TA18-074A.

[12] Daniel Voltz, *U.S. charges, sanctions Iranians for global cyber attacks on behalf of Tehran,* Reuters (Mar. 23, 2018), www.reuters.com/article/us-usa-cyber-iran/u-s-charges-sanctions-iranians-for-global-cyber-attacks-on-behalf-of-tehran-idUSKBN1GZ22K.

innocuous—such as revealing the names of UREs involved in a remediated NOP—can result in unintended consequences. In some instances, a URE may have remediated a particular instance of regulatory noncompliance. However, that URE may have experienced similar noncompliance—which occurred not because they are not committed to security, but because there are significant other factors at play (e.g., legacy systems, equipment compatibility). More importantly, however, while a particular URE has addressed a particular compliance issue or vulnerability, other entities may have not yet discovered or fixed a similar issue or vulnerability.

UREs face challenges in integrating modern information technology systems with older operational technology systems that were never designed with modern cybersecurity needs in mind. Sophisticated bad actors, like the ones discussed above, may be able to discern points of attack and vulnerabilities in publicly disclosed UREs based on information discerned from NOPs—especially when such information is coupled with other publicly available information. The Trade Associations recognize that public access to information is important, and appreciate the goal of FOIA, but believe the line must be drawn where a requested disclosure could have a negative impact on reliability and security of the bulk-power system.

Commission staff must determine that any new information—which staff is considering releasing—cannot be useful to a person planning an attack on the bulk-power system.

The Commission is responsible for protecting "the reliability of the high voltage interstate transmission system through mandatory reliability standards." As a part of this role, the Commission seeks to "promote the development of safe, reliable, and secure infrastructure that serves the public interest."[13] In its strategic plan, the Commission acknowledges that jurisdictional infrastructure is at "increased risk from new and evolving threats, including physical and cyber security threats, by sophisticated perpetrators that often have access to significant resources."[14] To protect reliability, the Commission and its staff must determine whether the information it gathers from registered entities and produces in carrying out its enforcement of the reliability standards could be useful to a person planning an attack if the information was made public. Commission staff should consider and give deference to the data and information classifications provided by registered entities or, in this case, the UREs—who are required to give their sensitive information regarding security vulnerabilities and measures to NERC and FERC—to provide details on why the Commission should not release this information. Additionally, the Commission can consult with NERC staff regarding their proposed data and information classifications, which should also be given consideration and deference. Finally, it is significant that the Commission has its own subject matter experts (e.g., within the Office of Energy Infrastructure Security) who should be able to determine whether disclosure of information in response to FOIA requests would be useful to a person planning an attack on electric infrastructure. Further, Commission staff has at least 20 business days to conduct its own analysis through which it can consider and incorporate inputs from all of the above-referenced stakeholders.

[13] Federal Energy Regulatory Commission, Strategic Plan: FY 2018-2022 (Sep. 2018), https://www.ferc.gov/about/strat-docs/FY-2018-FY-2022-strat-plan.pdf?csrt=2040418639181005609, at 9.

[14] *Id.* at 14.

When performing its analysis of requested information, the Commission must consider not only the information requested (e.g., entity names) but information that is already in the public domain. For example, NERC has already published public versions of the NOPs on its websites for each of the dockets subject to the FOIA Request, which contain significant information that could become actionable with the addition of information that, alone, would be considered innocuous. In addition, Commission staff should evaluate other sources of information made public (e.g., by the entity's city and state), giving due consideration to the effect of that information if it was combined with the public NOP and the entity name to provide new information that would be useful to a person seeking to disrupt electric infrastructure.

In addition, Commission staff must consider whether other entities may not have yet discovered or fixed similar issues. The Commission should work with NERC and the UREs to ensure that there are no ongoing security issues related to the violations that might jeopardize security. This may be even more important if the Commission anticipates disclosing a particular NOP and its disclosure also plans to tie the NOP to the identification of a specific registered entity.

Commission staff should give due weight to NERC's technical expertise in deciding whether information related to the reliability standards should be protected as CEII.

In addition, Congress entrusted the Electric Reliability Organization ("ERO") or NERC with the technical expertise related to the reliability of the bulk-power system and therefore Commission staff should give due weight to NERC—the submitter in the FOIA Request—in determining whether disclosure of information regarding the violations of the CIP Standards might risk the security of the bulk-power system. In 2005, Congress delegated authority to the Electric Reliability Organization ("ERO") "to establish and enforce reliability standards for the bulk-power system," including requirements for cybersecurity protection.[15] In 2006, the Commission certified NERC as the ERO. Congress gave the Commission the authority to approve or disapprove such standards, but not to create them, recognizing that the ERO has the technical expertise necessary to develop reliability standards:

> The Commission shall give due weight to the technical expertise of the Electric Reliability Organization with respect to the content of a proposed standard or modification to a reliability standard and to the technical expertise of a regional entity organized on an Interconnection-wide basis with respect to a reliability standard to be applicable within that Interconnection. . .[16]

Congress also recognized the technical expertise of the ERO by giving the ERO the authority to conduct assessments of bulk-power system reliability and adequacy.[17] Furthermore, the purpose of the reliability standards, developed by NERC is "to provide for reliable operation of the bulk-power system." As a result, in determining whether specific information regarding the violations of the CIP Standards could jeopardize the security of the bulk-power system, Commission staff

[15] 16 U.S.C. § 824o (a)(2) – (3).

[16] *Id.* at (d)(2).

[17] *Id.* at (g).

should defer to NERC. If NERC objects to the release of the information requested in a FOIA request that is related to the reliability standards because it could be useful to a person in planning an attack on the bulk-power system, then Commission staff should continue to exempt this information under FOIA Exemption 3, unless staff sufficiently demonstrates that that the information cannot be useful to a person in planning an attack. Such a determination must be made by not only evaluating the information being considered for release, but also other information that has already in the public domain such as the public versions of the NOPs.

In conclusion, the Trade Associations recognize the delicate task before the Commission in balancing the public's need for information against the nation's need to protect itself from some of the gravest cyber threats in the world. We respectfully ask the Commission to deny Mr. Mabee's request. If the Commission decides to disclose any nonpublic information, then it must ensure that the disclosure of any of that information will not risk jeopardizing the security of the bulk-power system.

Respectfully submitted,

AMERICAN PUBLIC POWER ASSOCIATION
/s/ *Delia D. Patterson*
SVP Advocacy & Communications and General Counsel
2451 Crystal Dr., Suite 1000
Arlington, VA 22202
(202) 467-2900

EDISON ELECTRIC INSTITUTE
/s/ Emily Sanford Fisher
General Counsel and Corporate Secretary
701 Pennsylvania Avenue, NW
Washington, D.C. 20004
(202) 508-5000

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION
/s/ Randolph Elliott
Randolph Elliott
Senior Director, Regulatory Counsel
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-6818