UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards	)	Docket No. AD19-18-000

COMMENTS OF THE JOINT TRADE ASSOCIATIONS

These comments are jointly submitted by the Edison Electric Institute ("EEI"), the American Public Power Association ("APPA"), the National Rural Electric Cooperative Association ("NRECA"), the Large Public Power Council ("LPPC"), the Transmission Access Policy Study Group ("TAPS"), the Electric Power Supply Association ("EPSA"), WIRES, and the Electricity Consumers Resource Council ("ELCON") (together, the "Joint Trade Associations") in response to the *Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards* filed in this docket on August 27, 2019, by the staffs of the Federal Energy Regulatory Commission ("FERC" or "Commission") and the North American Electric Reliability Corporation ("NERC") ("White Paper").[1]

I. Introduction And Summary of Comments

The revisions to Notices of Penalties ("NOPs") proposed in the White Paper are intended to provide greater transparency about violations of Critical Infrastructure Protection ("CIP")

[1] Comments initially were due on September 27, 2019, but the Commission provided an extension in response to a Motion for Extension of Time to File Comments filed by EEI and other trade associations. As a result, comments are now due October 28, 2019.

Reliability Standards[2] by providing more information about the identity of registered entities ("REs") named in NOPs, while protecting details associated with the CIP Standards that were violated. While transparency may hold some value to the public and some stakeholders, it also can benefit malicious actors. Nonetheless, the revised NOP format proposed in the White Paper may satisfy the Commission's interest in transparency, while better protecting from disclosure information that is appropriately classified as CEII. In order to achieve these objectives, key modifications sought by the Joint Trade Associations are that:

- NERC work with REs and the Joint Trade Associations to share information with REs, similar to what has been provided in the past, in order to ensure that this information can continue to inform some RE compliance programs.
- Public NOP cover letters not disclose the particular Standards that may have been violated because this information, even without disclosure of the more detailed Requirements, can be used to better focus attacks on REs and the Bulk Power System ("BPS").
- The Commission recognize that there are circumstances in which the disclosure of the names of REs may compromise security, even once mitigation is complete.
- Consistent with the White Paper, the Commission establish a strong presumption disfavoring further disclosure of information related to the NOPs once RE names are disclosed, as such disclosure would severely compromise security.

A. Background

The White Paper represents the thinking of the Commission staff and NERC staff on NERC's submission, and the Commission's processing, of NOPs for violations of CIP Standards. These Standards include Requirements intended to support the cybersecurity of the BPS through both cyber and physical security measures.

To address concerns related to Freedom of Information Act ("FOIA") requests for information contained in NOPs, the joint staffs propose a new filing format: NERC would

[2] Herein, referred to as "CIP Standards" or "Standards."

include a public cover letter that discloses the RE name, the Standard(s) that were violated, and the amount of the penalty imposed. All other information in the NOP would be submitted as a non-public attachment for which NERC would request a designation as CEII. CEII is exempt from disclosure under FOIA.[3] Accordingly, the White Paper further represents that "[w]hile the names of violators would be made public with each CIP NOP submission, detailed information that could be useful to a person planning an attack on critical infrastructure, such as details regarding violations, mitigation and vulnerabilities, would likely be considered by Commission staff to be exempt from FOIA."[4]

This represents a change from current practice in two respects. First, under current practice, RE names and other details about the CIP Standard violations are not made public. Second, under current practice, REs have access to NOPs that have been redacted to protect CEII. The White Paper states that the proposed revised filing format would appropriately balance concerns about security related to disclosure of CEII and transparency.

B. Joint Trade Associations

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for about 220 million Americans and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. EEI's members are committed to providing affordable and reliable electricity to customers now and in the future. EEI's members include Generator Owners and Operators, Transmission Owners and Operators, and other entities subject to the

---

[3] *See* Fixing America's Surface Transportation Act ("FAST Act"), Pub. L. No. 114-94, § 61003 (specifically exempting the disclosure of CEII and establishing the applicability of FOIA exemption 3, 5 U.S.C. § 552(b)(3), which bars disclosure under FOIA of material that is protected under other federal law).

[4] White Paper at 4.

mandatory Reliability Standards developed by NERC and enforced by NERC, the Regional Entities, and the Commission. Accordingly, EEI members are directly affected by proposal set forth in the White Paper.

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 percent 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 NERC mandatory reliability standards.

NRECA is the national trade association representing nearly 900 local electric cooperatives operating in 48 states. America's electric cooperatives power over 20 million businesses, homes, schools, and farms across 56 percent of the nation's landmass and serve one in eight (42 million) consumers. NRECA's member cooperatives include 62 generation and transmission ("G&T") cooperatives and 831 distribution cooperatives. The G&T cooperatives generate and transmit power to distribution cooperatives that provide it to the end-of-the-line co-op consumer-members. Collectively, G&T cooperatives provide power to nearly 80 percent of the nation's distribution cooperatives. The remaining distribution cooperatives receive power from other generation sources. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service. NRECA's member cooperatives include cooperatives that are REs with compliance obligations under Reliability Standards established by NERC. Therefore, the Joint Staff White Paper's proposals will directly affect NRECA's member cooperatives and their consumer-members.

LPPC is an association of the 27 largest state-owned and municipal utilities in the nation and represents the larger, asset-owning members of the public power sector. LPPC members are

also members of APPA and own approximately 90 percent of the transmission assets owned by non-federal public power entities.

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states promoting open and non-discriminatory transmission access.[5] Representing entities entirely or predominantly dependent on transmission facilities owned and controlled by others, TAPS has long recognized the need for reliable and secure transmission infrastructure that enables TAPS members to serve their load affordably. As TDUs, TAPS members make investments to secure their own assets and pay, through transmission rates, for investments made by other utilities to improve their transmission facilities' security. In addition, many TAPS members participate in the development of and are subject to compliance with NERC reliability standards, including CIP standards.

EPSA is the national trade association representing leading independent power producers and marketers. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. Power supplied on a competitive basis collectively accounts for 40 percent of the U.S. installed generating capacity. EPSA seeks to bring the benefits of competition to all power customers. The comments contained in this filing represent the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.

WIRES is an international non-profit trade association of investor-, publicly-, and cooperatively owned transmission providers, transmission customers, regional grid managers, and equipment and service companies. WIRES promotes investment in electric transmission and

[5] David Geschwind, Southern Minnesota Municipal Power Agency, chairs the TAPS Board. Jane Cirrincione, Northern California Power Agency, is TAPS Vice Chair. John Twitty is TAPS Executive Director.

progressive state and federal policies that advance energy markets, economic efficiency, and consumer and environmental benefits through development of electric power infrastructure.

ELCON is the national association representing large industrial consumers of electricity. ELCON member companies produce a wide range of products from virtually every segment of the manufacturing community. ELCON members operate hundreds of major facilities and are consumers of electricity in the footprints of the organized markets. Reliable electricity supply at just and reasonable rates is essential to our members' operations.

II. NOTICE AND COMMUNICATIONS

All notices and communications with respect to this proceeding should be directed to the representatives listed below:

Megan Vetula
Associate General Counsel, Energy Regulation
Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, D.C. 20004
(202) 508-5000
mvetula@eei.org

John E. McCaffrey
Regulatory Counsel
American Public Power Association
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
jmccaffrey@publicpower.org

Randolph Elliott
Senior Director, Regulatory Counsel
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-6818
randolph.elliott@nreca.coop

Rebecca J. Baldwin
Cynthia S. Bogorad
Spiegel & McDiarmid LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000
cynthia.bogorad@spiegelmcd.com
rebecca.baldwin@spiegelmcd.com

Jonathan Schneider
Jonathan Trotta
Stinson LLP
1775 Pennsylvania Ave., NW, Suite 800
Washington, D.C. 20006
(202) 785-9100
jonathan.schneider@stinson.com
Jonathan.Trotta@stinson.com

Nancy Bagot
Bill Zuretti
Electric Power Supply Association
1401 New York Ave., NW, Suite 950
Washington, DC, 20005
202-628-8200
nancyb@epsa.org
bzuretti@epsa.org

Brian Gemmell
WIRES
40 Sylvan Rd, Waltham
National Grid
Waltham, MA 02451-11220
(617) 833-1261
Brian.Gemmell@nationalgrid.com

Devin Hartman
President and CEO
Electricity Consumers Resource Council
1101 K Street, NW, Suite 700
Washington, DC 20005
(202) 682-1390
dhartman@elcon.org

The Joint Trade Associations request waiver of 18 C.F.R. § 203.(b)(3) to permit more than three persons to receive communications in this proceeding.

III. COMMENTS

A. Electric Utilities Have Every Incentive to Protect the Reliability of the BPS; The White Paper Does Not Articulate A Compelling Rationale for the Disclosure of Information Contained in NOPs.

The Joint Trade Associations' members provide safe, affordable, reliable and secure electric service to their customers. The power sector is the only sector for which there are mandatory CIP Standards. The power sector is committed to compliance with these and other standards, as violations not only are subject to significant fines, but also could undermine the provision of reliable service to customers. This commitment to reliable electric service and compliance with all reliability standards is underscored by the fact that the clear majority of the NOPs reported by NERC to the Commission are the result of self-reporting by registered entities. Disclosure of the names of those entities making self-reports will not further increase or incent compliance.

Given the highly technical nature of the BPS and its operations, it is not clear whether there is a benefit to the security and reliability of the BPS if CEII or other information in the NOPs were made public. While various parties, including the Commission and NERC in the White Paper, have asserted that transparency is a goal of the revised NOP format, the White Paper does not articulate a clear or compelling reason why an interest in transparency outweighs the associated security risk, recognizing that incremental disclosure of CEII creates additional risk that adversaries can use to better target their attacks on a specific entity or to take advantage of trends or other vulnerabilities. There may be value in providing the public with some

additional information about CIP Standard compliance, but this should not come at the expense of ensuring a reliable and secure BPS.[6]

B. CIP NOPs Are CEII and Must Not Be Shared Publicly; NERC Should Work with Registered Entities to Share Securely Information Needed to Develop and Implement Effective Compliance Programs.

If the Commission were to adopt the proposed NOP format, the details that currently are released in the public versions of the NOPs must be treated as confidential and protected from public disclosure. Although the current NOP format provides information about potential violations and mitigation options some members of the Joint Trade Associations find valuable, NOP CEII must be protected, particularly if the RE name has been disclosed. As noted in the White Paper, disclosing the name of the entity makes the detailed information that would be in the confidential NOP even more valuable to would-be attackers and makes it even more important that this information be protected from public disclosure.

NERC has the technical resources, tools, and a history of effectively communicating BPS cyber risks to the electric industry. NERC and the entire industry use several mechanisms to collect cyber risk information, including collecting and analyzing information contained in NOPs. Members of some of the Joint Trade Associations review all NOPs on a regular basis as a part of their internal controls and use the information to improve their own reliability, security, and compliance practices. If the proposed NOP format were to be adopted, these REs would lose this opportunity to learn from each other about cyber vulnerabilities and associated mitigation measures. NERC should therefore engage with REs and the Joint Trade Associations to continue

[6] In response to the Submitter's Rights Letters sent to several EEI members earlier this year, EEI filed comments with the Commission outlining the risks to the BPS that would be created by disclosing CEII. These letters are attached as Appendices A and B.

sharing with REs, in a secure way, information similar to what has been provided in the past to develop and implement effective compliance programs.

C. The Revised NOP Format Should Not Specify the CIP Reliability Standards Violated; Such Information Could Be Used to Better Target Attacks on Named Entities.

The proposed revised NOP format would disclose the CIP Reliability Standards violated but would not disclose the Requirements under those Standards.[7] The White Paper does not provide a reason for making public the Standard violated, other than referencing the goal of being more transparent about CIP NOPs, and implies that information about the violated Standard is less sensitive than other information that would be contained in the non-public NOP.[8] The value to the public in providing information about the Standard violated is greatly outweighed by the increased risks to BPS security because public disclosure would allow adversaries to better target attacks on named entities. The Commission should not adopt a revised NOP format that would disclose information about the Standard violated.

The White Paper erroneously assumes that identification of the Standard violated, without further identification of the specific Requirements, will not create an increased risk of cyberattack. To begin with, certain of the Standards have a narrow subject area, with correspondingly few Requirements, such that disclosure of the Standard is itself revealing. Further, the White Paper does not address instances in which the NOP covers violations of a single Standard and how this information could be used by sophisticated actors. For example, if the only Standard violated identified in the NOP cover sheet is CIP-005-5, Electronic Security Perimeters, a potential adversary would know to target attacks on firewalls at a specific RE. In

---

[7] *See* White Paper at 3.

[8] *See id.*

these instances, identification of the Standard would provide useful, actionable information to the potential attackers. Further, disclosure of the Standard violated combined with knowledge that the violation had been mitigated, can signal to sophisticated adversaries that their exploits have been discovered, encouraging the development of new efforts to attack the BPS.

Given that the public would require specialized training and expertise to derive any value from the name of the Standard violated (beyond the general understanding that a Standard was violated), it is not clear what benefit there is in automatic disclosure of this information. To better protect BPS reliability, reference to specific Standards should not be included in the NOP public cover sheet.

D. If the Commission Discloses Entity Names, NOP Information Must Be Presumed to Be CEII and Protected from Disclosure.

With disclosure of the identities of REs pursuant to the White Paper, the Commission should establish a strong presumption disfavoring further disclosure of information related to the NOPs. In indicating that disclosure beyond that contemplated through NERC's public letter is not "likely," the White Paper acknowledges that the combined disclosure of the name of an RE along with the substance of the NOP poses a substantial security risk, by enabling bad actors to focus attacks on entities with known, publicly detailed, vulnerabilities.[9] Accordingly, the Commission should establish a strong presumption that upon filing of the proposed NOP public cover sheet, further substantive information contained in the NOP is CEII, appropriately exempt from FOIA disclosure.

E. The Commission Should Recognize that Entity Names Can Be CEII that Should Be Protected from Disclosure Under FOIA.

[9] *See id.* at 11-12.

The proposed revised NOP format would disclose the name of every entity for which NERC files an NOP with the Commission. For many reasons, the disclosure of RE names makes those entities a target. As discussed above, the threat of the disclosure of names is not needed to incent compliance with CIP Standards. Moreover, as the White Paper acknowledged, disclosure of names will increase attacks on those entities.[10] More importantly, however, the disclosure of RE names makes it even more critical that the Commission protect from disclosure other information in NOPs so as to mitigate this increased risk of attack.[11] If, however, the Commission determines that the default should be to disclose entity names, there should be provision for NERC to request that some names be treated as CEII and protected from disclosure.

The White Paper proposed that NERC would only file CIP NOPs after mitigation of the underlying violation is complete, thus minimizing the possibility of adversarial insight resulting from the disclosure of any name.[12] While it is appropriate to file NOPs after mitigation has occurred in an effort to minimize the likelihood of success of attacks aimed at the identified entity, this delay may not provide meaningful protection from increased harm in all cases. The knowledge that named REs have mitigated NOP violations will not discourage malicious actors from probing the cyber security defenses of those entities. Malicious actors look for the weak link in the electricity sector's cyber security defenses, and they may believe NOP disclosure provides them a list of potential targets with lower defenses. Anecdotally, Joint Trade

---

[10] *See id.* at 11.

[11] *See id.* at 10 ("...the name of the [entity], coupled with the public information usually contained in CIP NOPs, would reasonably provide useful information to a person planning an attack on critical infrastructure").

[12] *See id.* at 11.

Association members that have had their names disclosed have noticed an increase in the number of attempted attacks.

Further, depending on the nature of the violation and the Standard violated, NERC may still have reason to believe that the risks of disclosure are too great. Other circumstances surrounding the violations may also warrant that RE names be protected to mitigate risks to the BPS. While speculating as to these circumstances in advance of such situations is of little value, the Commission should recognize that such circumstances may exist and prepare for NERC to request CEII treatment of RE names, supported by sufficient evidence so that FERC can make such a designation if needed.

The White Paper does recognize that an entity name might justifiably be designated as CEII in certain circumstances, but limits these to an actual Cybersecurity Incident.[13] The Commission offers no factual basis for limiting the disclosure of a name as CEII to those instances involving an actual Cybersecurity Incident—since no cyber events that caused interruptions of electrical system operations have ever been reported—and should not constrain potential NERC requests for such treatment. Instead, if the Commission moves to implement the revised NOP format, FERC should ensure that NERC and the RE in question have an opportunity and a process to seek CEII designations for names that would otherwise be included in the public cover sheet. Further, consistent with its regulations, the Commission should commit in these instances to treating the entity name as confidential until a formal CEII designation is made.

More importantly, as noted in the White Paper and discussed in more detail below, the Commission must make it clear in any final action on this proposal that the disclosure of RE

[13] *See id.* at n.24.

names in the proposed NOP cover sheet requires that the Commission protect NOP details from disclosure. The disclosure of names increases the value of this information to those who seek to harm reliability and, therefore, increases risk.

F. Disclosing Penalty Amounts Can Create Risk and Confusion.

The revised NOP format would include the amount of the penalty on the public NOP cover sheet.[14] Current practice discloses penalty amounts but does not disclose the name of the entity. While penalty amounts are not CEII, they can create some risk, as well as significant confusion for the public. The Commission should evaluate how it provides penalty information in an effort to minimize this risk and confusion.

The amount of the penalty can signal the magnitude of the violation, which in turn can encourage attackers to focus on certain named REs over others. In other instances, however, the penalty amount may be unrelated to the magnitude or severity of the violation. While the public may think of the penalty amount as some sort of proxy for the severity of the violation, the penalty often just reflects the cumulative impact of a series of smaller, less serious violations over a relatively longer period of time. The penalty also may be subject to negotiation and settlement, further limiting the usefulness of the amount in the relative evaluation of entities' compliance performance. If one goal of the proposed revised NOP format is transparency, the Commissions should consider whether such transparency is useful to the public.

G. If the Commission Moves Forward with the Revised NOP Format, the Commission Should Undertake a Rulemaking Addressing CEII.

The Commission should be more transparent in how it determines what information is CEII that is exempt from disclosure. Current regulations merely cite the definition of CEII but

[14] *See id.* at 10.

provide no information about how the Commission applies this definition. And, the White Paper merely states that the Office of External Affairs consults with the relevant experts.[15] In recent Notices of Intent to Release CEII, the Commission appears to have assessed several factors, including: the nature of the CIP violation; whether mitigation is complete; the content of the public and non-public version of the NOP; whether an audit had occurred since the violation(s); whether the violations were administrative or technical in nature; and the length of time that has elapsed since the NOP was filed. These factors may be important in determining whether a piece of information is CEII, but there may be other factors that should be considered, and it would be helpful to understand how and whether the Commissions weighs or ranks these factors. To complement the proposed NOP format, FERC also should undertake a rulemaking to take comment from all stakeholders on the appropriate factors to be considered (and their relative weights) when making a CEII determination.[16]

Moreover, in undertaking such a rulemaking—and when making any CEII determination—the Commission should ensure that the relevant inquiry is not whether information could or should be disclosed to a FOIA requestor or the public more generally, but whether specific information is CEII and therefore must be protected. When addressing requests for release of confidential NOP information, the Commission should keep in mind the careful balance between disclosure and nondisclosure that Congress articulated in FOIA.

H. FERC Also Should Address Existing FOIA Requests for NOPs and CEII Contained in Those NOPs.

[15] *See id.* at 3 n.3.

[16] It would be more appropriate for the Commission to issue a Notice of Proposed Rulemaking on the topic of FOIA and CEII than to schedule a public hearing on this topic, as some have requested in this administrative docket.

In the White Paper, the joint staffs note that the proposed revisions to the NOP format would not apply to any existing FOIA requests.[17] As discussed in the White Paper, there are hundreds of outstanding FOIA requests for previously filed NOPs. These requests seek not only the sensitive information that the proposed revised NOP format would make public going forward—the names of registered entities, the Standards violated, and amounts of the penalties imposed—but also more detailed information, much of which is likely to be CEII. The requestors assert that providing this detailed information is important for the sake of transparency and that such transparency will increase the security of the electric grid. Despite these assertions, requestors cannot explain how providing such information to the public actually would serve to increase the security of the BPS. They cannot explain this because the detailed information included in NOPs is not meaningful to the general public as it is highly technical and requires specialized training and expertise to understand.[18] The public cannot take action on this information. But, would-be attackers, who do have such training and expertise, can use this information to target specific electric utilities and the BPS in general. In the White Paper, the joint staffs recognize that providing the name of the registered entity coupled with the detailed violation information increases the risks of attack and undermines the goals of the CIP Standards.[19]

Accordingly, the Commissions should continue to carefully consider disclosing existing NOP information to FOIA requestors and should continue to ensure that submitters and others have sufficient opportunity to explain why the information requested should be designated as

---

[17] *See* White Paper at 4.

[18] Even basic information like the name of the company that is the subject of the NOP does not provide a FOIA requestor with information that they could use to help protect the energy grid from cyberattacks.

[19] *See* White Paper at 3, 10.

CEII. And, the Commission should rely on all possible FOIA exemptions to minimize threats to reliability and security by protecting information about critical infrastructure from disclosure, which are discussed in more detail below.

1. Consistent with the Commission's Regulations, Submitters and UREs Should Continue to Be Given Ample Time to Respond to FOIA Requests

Given the risks created by disclosure of information contained in the existing NOP format, the Commissions should continue to carefully evaluate FOIA requests for this information. NERC has requested CEII treatment for much of this information and the Commission should so designate any information that could reasonably provide useful information to a person planning an attack on critical infrastructure and then, consistent with the FAST Act, protect that information from disclosure. If the Commission requires additional information to determine whether NOP information that is subject to a FOIA request is CEII, the Commission should continue providing not only the submitter (NERC), but also the unidentified registered entity ("URE") ample time to provide additional support to the Commission.

FERC's regulations addressing requests for CEII state that submitters should be provided *at least* five business days to respond before any information is disclosed.[20] FERC's notices to NERC and UREs have often requested responses in five days (or less, given the timeliness of notices). The Commission, consistent with its own regulations, should err on the side of caution and provide at least five business days if not considerably more. The Commission also should ensure that UREs are notified at the same time as NERC of FOIA requests and are given as much time as NERC to respond. Given the risk of harm to the security of the BPS, there is no need to rush to respond to these FOIA requests.

[20] *See* 18 C.F.R. § 388.113(d)(1)(vii) (2019) (emphasis added).

2. The Commission Should Clarify the Duration of a CEII Designation and the Process for Designation Extensions.

FOIA requestors have asserted that any CEII designations for information submitted more than five years from the date of their request have expired, eliminating the protection from disclosure provided by the FAST Act. This is clearly contrary to the Commission's regulations, which state that information is treated as confidential until the Commission has reason to make a CEII designation; the request for CEII designation is not the same as a Commission designation to that effect.[21] After making such a determination, the designation has a duration of five years, but this designation can be extended.[22]

To further protect CEII from disclosure, the Commission should take several steps. First, the Commission should clarify that the expiration of any CEII designation is not measured from the date that NERC (or another entity) submits a request to treat information as CEII, but from the date that such a designation is made by the Commission. Second, the Commission should ensure, upon the expiration of a CEII designation, that both the submitter and the URE are provided as least five business days to seek, and provide support for, an extension of that designation for an additional period.[23] Finally, the Commission should make clear to any FOIA requestor that information designated as CEII will continue to be treated as non-public until the Commission makes an official determination to un-designate that information, consistent with existing regulations.[24]

---

[21] *See id.* at § 388.113(d)(1)(iv); *see also* White Paper at 7.

[22] *See id.* at § 388.113(e). But, note that the Commission's regulations appear to allow a requestor to seek a CEII designation that would last longer than five years and that the Commission could designate material as CEII for a longer period. *See* 18 C.F.R. at § 388.112(d)(1)(i).

[23] *See id.* at § 388.113(e)(4).

[24] *See id.* at § 388.113(e)(3).

I. There is Strong Legal Support for Not Disclosing CEII, Whether It is Contained in NOPs that Use the Proposed New Format or Not.

If the Commission determines that information is CEII, there is strong legal support that this information should not be disclosed under FOIA. A very recent U.S. Supreme Court decision is particularly instructive. For many years, federal courts took the position that because FOIA was a disclosure statute, its exemptions—which allow agencies some discretion to withhold certain types of information—should be narrowly construed. That approach often led agencies and courts to improperly restrict the scope and applicability of FOIA's exemptions in favor of disclosing information.

In its June 2019 decision in *Food Marketing Institute v. Argus Leader Media*, the Supreme Court soundly rejected that approach. 139 S. Ct. 2356, 2366 (2019). The Court emphasized that FOIA exemptions should not be narrowly construed but must instead be given a "fair reading." *Id.* (citing *Encino Motorcars, LLC v. Navarro*, 584 U.S. ---, 138 S. Ct. 1134, 1142 (2018)). FOIA's exemptions are just as important to FOIA's function and purpose as its disclosure requirements, and agencies and courts err when they read limitations into the exemptions not present in the statutory text. The Court emphasized that "just as we cannot properly *expand* [a FOIA exemption] beyond what its terms permit, we cannot arbitrarily *constrict* it either by adding limitations found nowhere in its terms." *Id.* (interpreting Exemption 4) (citing *Milner v. Dep't of Navy*, 562 U.S. 562, 570-71 (2011)).

Even if the Commission opts not to conduct a rulemaking to better articulate the factors to be assessed when determining whether information is CEII, the Supreme Court's guidance should inform the Commission's approach to such designations: rather than looking for ways to increase disclosure of NOP information that may be CEII, the Commission should instead begin with an appropriate application of existing FOIA law and should seek all possible protection

from disclosure for this information. In fact, three FOIA exemptions apply to information contained within CIP NOPs, each of which is sufficient to protect this information from disclosure. As the Supreme Court indicated in its *Food Marketing Institute* decision, the Commission must give a fair reading to these exemptions. Not even FOIA, a disclosure statute, requires disclosure at all costs. FOIA's exemptions are integral to the balance of disclosure against nondisclosure that Congress sought to achieve.

1. Exemption 3

FOIA Exemption 3 allows the government to withhold from disclosure information specifically exempted from disclosure by statute "if the statute affords the agency no discretion on disclosure, or establishes particular criteria for withholding the data, or refers to particular types of information to be withheld."[25]

The FAST Act is clearly such a statute. It provides that "critical electric infrastructure information" "shall be exempt from disclosure under section 552(b)(3) of Title 5"; and "shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision or tribal law requiring public disclosure of information or records."[26] Significantly, when it defined "critical electric infrastructure information" Congress did not adopt the Commission's definition of "critical energy infrastructure information;" instead, Congress provided that "critical electric infrastructure information" includes "critical energy infrastructure information" but extends beyond the meaning of that narrower category.

> "Critical electric infrastructure information" is defined as:
>
> [I]nformation related to critical electric infrastructure, or proposed critical electrical infrastructure, generated by or provided to the Commission or other Federal agency,

[25] *Baldrige v. Shapiro*, 455 U.S. 345, 352-53 (1982); *see also* 5 U.S.C. § 552(b)(3) (2012).

[26] 16 U.S.C. § 824*o*-1(d)(1).

> other than classified national security information, that is designated as critical electric infrastructure information by the Commission or the Secretary pursuant to subsection (d). Such term includes information that qualifies as critical energy infrastructure information under the Commissions regulations.[27]

"Critical electric infrastructure," in turn, is defined as:

> [A] system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters.[28]

The statutory scheme thus affords the Commission and the Secretary no discretion on exemption from disclosure of critical electric infrastructure information, while charging the Commission (or the Secretary), with designating such information as CEII. In 2016, FERC did just that, defining CEII as:

> [S]pecific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:
> (i) Relates details about the production, generation, transportation, transmission, or distribution of energy;
> (ii) Could be useful to a person in planning an attack on critical infrastructure;
> (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
> (iv) Does not simply give the general location of the critical infrastructure.[29]

It is important to recognize that Congress gave the Commission much broader authority to protect critical electric infrastructure information than reflected in FERC's implementing rules. The FAST Act would allow the Commission to grant a categorical designation of cyber security information as critical electric infrastructure information exempt from disclosure under FOIA, for example, but the Commission's rules do not provide for a categorical designation. The Commission should revise its regulations to establish procedures for a categorical designation of

---

[27] *Id.* at § 824*o*-1(a)(3)(emphasis added).

[28] *Id.* at. § 824*o*-1(a)(2).

[29] 18 C.F.R. § 388.113(c)(2).

cyber security information as critical electric infrastructure information.[30] Because the Department of Energy is a national security agency, the Secretary may be in a better position than the Commission to assess cyber security threats and the need to act with dispatch to protect cyber security information from disclosure. And if greater transparency proves to jeopardize cyber security by identifying targets for malicious actors, it is possible the Commission may want to act quickly to restore defenses. Establishing a process for categorical designation does not mean that such a designation will occur, it only allows for rapid action to protect cyber security information if the need arises.

The White Paper proposes that future submissions will consist of a public cover letter containing the name of the violator, the CIP Standard(s) violated (but not the Requirement), and the penalty amount. As discussed above, whether this information "could be useful to a person in planning an attack on critical infrastructure" is debatable and the Commission should ensure that this information is not CEII before mandating its disclosure.[31] On the other hand, the remainder of the CIP NOP filing, containing details on the nature of violation, mitigation activity, and potential vulnerabilities to cyber systems *do* "relate details about the production, generation, transportation, transmission, or distribution of energy," and certainly "could be useful to a person in planning an attack on critical infrastructure."[32] Therefore, the Commission must not make this information available to the public in any form and can legitimately withhold such information in response to a FOIA request.

---

[30] Id. at. § 824*o*-1(d)(3).

[31] 18 C.F.R. § 388.113(c)(2). Note that while 18 C.F.R. § 388.113(c)(2)(iii) appears to list exemption from FOIA as a *requirement* for deeming information CEII, it is more likely that exemption from FOIA is a *result* of information being deemed CEII. Otherwise, information could only be exempt from FOIA if it was already exempt from FOIA, a circular definition unlikely to be Congress's intent.

[32] *Id.*; White Paper at 3.

2. Exemption 7

CEII in the non-public CIP NOP filings may be withheld pursuant to FOIA Exemption 7(F), as "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information [...] (F) could reasonably be expected to endanger the life or physical safety of any individual."[33]

The threshold inquiry under Exemption 7(F) is whether the information was compiled for law enforcement purposes. Because the information here relates to CIP NOPs, which are generated as a result of violations of CIP Standards, the information is appropriately considered to be collected for law enforcement purposes. As Justice Alito wrote in his concurrence in *Milner*, "[c]rime prevention and security measures are critical to effective law enforcement as we know it."[34] Because the information is being collected to reduce infrastructure vulnerability to crime and acts of terrorism, it also qualifies as collected for law enforcement purposes under the statute.[35]

The second question under Exemption 7(F) is whether release of this information "could reasonably be expected to endanger the life or physical safety of any individual."[36] The D.C. Circuit has held that it is not necessary for the government to identify particular individuals before the fact in order to meet the requirements of this exemption.[37] The CEII here implicates individual physical safety. An attack on Critical Electric Infrastructure could disrupt electrical

---

[33] 5 U.S.C. § 552(b)(7).

[34] 562 U.S. at 583 (Alito, J., concurring).

[35] *See Pub. Employees for Envt'l. Responsibility v. U.S. Section, Int'l Boundary & Water Com'n, U.S.-Mexico*, 740 F.3d 195, 204 (D.C. Cir. 2014) ("[P]reventing dam attacks and maintaining order and ensuring dam security during dam emergencies qualify as valid law enforcement purposes under the statute. Because the emergency action plans and the inundation maps were created in order to help achieve those purposes, among others, they were 'compiled for law enforcement purposes.'").

[36] 5 U.S.C. § 552(b)(7)(F).

[37] *Elec. Privacy Info. Ctr. v. U.S. Dept. of Homeland Security*, 777 F.3d 518, 525 (D.C. Cir. 2015).

services to millions of Americans, including vulnerable populations whose safety depends on reliable electricity.

In applying Exemption 7, the government must also adhere to the FOIA Improvement Act of 2016, which added a new requirement that an agency must "reasonably foresee[] that disclosure would harm an interest protected by an exemption."[38] The 2016 Amendment codifies longstanding Department of Justice practice to encourage agencies to withhold only information that complies with the spirit of the exemptions, rather than withhold all information that technically fits within an exemption.[39] But the information contained in the proposed non-public attachments to the CIP NOPs surely is the type of information intended to be protected by Exemption 7(F). Its release would endanger individuals, and the government intends to withhold the information to protect the BPS and consequently all people who rely on it.

3. Exemption 4

Finally, the proposed changes to CIP NOP submissions also implicate FOIA Exemption 4. Exemption 4 protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."[40] The Supreme Court examined Exemption 4 most recently in *Food Marketing Institute*.[41] Information is "confidential" for the purposes of Exemption 4 "[a]t least where commercial or financial information is both customarily and actually treated as private by its owner and provided to the government under an assurance of privacy."[42]

---

[38] 5 U.S.C. 552(a)(8)(A)(i).

[39] *See* 162 Cong. Rec. H3717 (daily ed. June 13, 2016); *see also* Memorandum from Eric Holder, Atty. Gen. of the U.S., to Heads of Depts. & Agencies Regarding the Freedom of Information Act (Mar. 19, 2009).

[40] 5 U.S.C. § 552(b)(4).

[41] 139 S. Ct. 2356 (2019).

[42] *Id.* at 2366.

The Commission's historical confidential treatment of NOP information qualifies as an adequate assurance of privacy to invoke Exemption 4. If implemented, the revised format proposed in the White Paper similarly constitutes an assurance of privacy as to the nonpublic portion of the submission.[43] Moreover, any information submitted by regulated entities as part of the NOP process—*even if the information does not rise to the level of CEII*—should be withheld under Exemption 4 if the information is customarily and actually treated by the submitter as private. Submitters may have enforcement rights to protect this information under the Administrative Procedure Act and the Trade Secrets Act.[44]

IV. CONCLUSION

The Commission and NERC expended significant energy developing the White Paper. The Joint Trade Associations appreciate the opportunity to provide comments that we hope will the Commission in the shared mission to protect U.S. national security by more effectively balancing the safety and security of the nation with transparency. The Joint Trade Associations' members are committed to working with one another, the Commission, and NERC to protect the nation's energy grid from cyberattacks. The Joint Trade Associations look forward to continued engagement with the Commission and NERC on this important topic.

---

[43] *Cf. id.* at 2363 (citing 43 *Fed. Reg.* 43,275 as an assurance of privacy, which states "The contents of applications or other information furnished by firms . . . may not be used or disclosed to anyone . . . .").

[44] *See Chrysler v. Brown*, 441 U.S. 281 (1979).

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

/s/ Emily Sanford Fisher
Emily Sanford Fisher
General Counsel & Corporate Secretary

AMERICAN PUBLIC POWER ASSOCIATION

/s/ John E. McCaffrey
John E. McCaffrey
Regulatory Counsel

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

/s/ Randolph Elliott
Randolph Elliott
Senior Director, Regulatory Counsel

LARGE PUBLIC POWER COUNCIL

/s/ Jonathan Schneider
Jonathan Schneider
Counsel

TRANSMISSION ACCESS POLICY STUDY GROUP

/s/ Rebecca J. Baldwin
Rebecca J. Baldwin
Counsel

ELECTRIC POWER SUPPLY ASSOCIATION

/s/ Nancy Bagot
Nancy Bagot
Senior Vice President

WIRES

/s/ Brian Gemmel
Brian Gemmel
President

ELECTRICITY CONSUMERS RESOURCE COUNCIL

/s/ Devin Hartman
Devin Hartman
President & CEO

October 28, 2019

Appendix A

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-2019-19

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 January 18, 2019 Submitter's Rights Letter to Mr. Kichline 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 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 North American Electric Reliability Corporation ("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.

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

[1] FOIA No. FY19-019 (January 18, 2019).

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 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 six dockets, [2] but the actual request seeks public disclosure of the Full NOPs and "Spreadsheet NOP." In addition, the requester has also submitted requests for the same information for not only these six dockets, but from 236 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. Also, this information has previously been protected by the Commission from public disclosure.[4] As discussed below, this is not a new policy, but one carefully crafted by the Commission over nine years ago in its 2011-2012 Find, Fix, and Track and Report ("FFT") proceeding—an open and transparent proceeding in which stakeholders and the public were able to weigh in on policy concerns, ultimately striking a careful balance between information disclosure and national security throughout the six months of that proceeding.[5] Disclosing the requested information in response to the underlying FOIA Request before the Commission would represent a significant change to the Commission's policy on the protection of such information related to the security of the Bulk-Power System. Due to the risks posed to national security, the Commission should not abrogate the process established in these previous proceedings in response to this or any other FOIA request. Instead, before contemplating such a change in policy, the Commission should provide all stakeholders an opportunity for notice and comment in a full rulemaking similar to the FFT proceeding.

The Trade Associations oppose the release of the requested documents because risks to the Bulk-Power System from disclosure far outweigh any benefit to the public from disclosure.

---

[2] FERC Docket Nos.: NP14-29-000, NP14-30-000, NP14-32-000, NP14-37-000, NP14-39-000, and NP14-41-000.

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

[4] Significant information on penalties and specific violations (e.g., specific standard and requirements) is made publicly available in the NOPs posted on NERC's website, but the more sensitive information (e.g., registered entity names and mitigation measures) has been protected from disclosure as privileged and confidential to protect public safety and security.

[5] *See* FFT Order, 138 FERC ¶ 61,193 (Mar. 15, 2012).

Security threats to utility systems and the Bulk-Power System continues to grow. For example, in the last year, the following has occurred:

1. 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 US utilities.[6]

2. The United States Department of Justice indicted foreign hackers who successfully penetrated hundreds of US 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.[7]

In other words, 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. The FOIA request to publicize sensitive information about the U.S. electric grid could—as FERC noted earlier—assist these terrorists and nation-states in attacking the U.S. grid. Even information that some may deem innocuous—such as revealing the names of UREs involved in a remediated NOP—can result in unintended consequences. For example, in some instances, a URE may have remediated a particular instance of regulatory noncompliance. However, that URE may have experienced a pattern of similar noncompliance—not because of a lack of will to fix, but because there are significant other factors at play. In addition, 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 their patterns of NOPs. 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 might risk the security of the Bulk-Power System.

The release of the 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

---

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

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

such information "could reasonably be expected to endanger the life or physical safety of any individual."[8]

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."[9] 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, which the Commission has consistently protected from public disclosure to prevent jeopardizing the security of the Bulk-Power System. This information provides details and strategic security information on 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.[10]

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 the critical cyber assets and the NERC CIP violations of the UREs treated in the dockets he has identified, 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.[11] In addition, FERC has previously responded to a similar request, determining that identification of an Unidentified Registered Entity ("URE") is protected from disclosure by 5 U.S.C. §§ 552(b)(3) and 7(f).[12] FERC's response letter noted that:

> with respect to the name of the Unidentified Registered entity, disclosing such name could provide 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.[13]

---

[8] 15 U.SC. §§ 552(b)(3) and 7(F).

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

[10] 18 C.F.R. § 388.109(c)(5).

[11] *See, e.g., Mandatory Reliability Standards for Critical Infrastructure Protection*, Order 706, 122 FERC ¶ 61,040 at P 330 (2008).

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

[13] *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

Accordingly, the release of the information requested is not required by FOIA because Exemptions 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 Exemptions 3 and 7(F), but it is reasonably foreseeable that disclosure would harm the security interests that the exemptions and the FAST Act explicitly protect.[14]

If the Commission decides to change its disclosure policy regarding the CIP Reliability Standards, then the Commission should first provide public notice and opportunity to comment.

The Trade Associations appreciate the delicate task before the Commission—to balance the need for public transparency with the need to protect national security and public safety. As described above, granting the FOIA request poses significant risks to public safety and national security and as discussed below, granting Mr. Mabee's FOIA request would constitute a sweeping policy change with respect to the Commission's protection of information related to the Bulk-Power System. Releasing the information requested in the current FOIA request would set precedent for future requests such as those made for the other 236 dockets without allowing the other affected entities adequate notice and time to comment on the consequences of such a change in policy and its potential detrimental impact to the security of the Bulk-Power System. If the Commission believes that disclosure may be warranted, then such a departure from longstanding Commission precedent should be considered in a public notice and comment proceeding, not in the context of a FOIA request that provides little notice to limited interested parties and an unrealistically short comment period.

In addition, the Commission has previously addressed many of the policy issues raised in the FOIA request. Specifically, in 2011, NERC submitted to this Commission for approval its FFT process "to more efficiently process and track lesser risk violations in order to focus their resources on issues that pose the greatest risk to reliability."[15] On March 15, 2012, the Commission issued the FFT Order approving this process.[16] The issue of publicly identifying registered entities was squarely addressed in the FFT Order.[17] The Commission held that while the identity of the entity generally would be provided, the exception enshrined in 18 C.F.R. § 39.7(b)(4) for violations that relate to "a Cybersecurity Incident or that would jeopardize the security of the Bulk-Power System if publicly disclosed. . . . [would] continue to apply in the

---

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.

[14] 18 18 C.F.R. § 388.109(c)(5).

[15] FFT Order, 138 FERC ¶ 61,193 at P 2.

[16] *Id.*

[17] *Id.* at P 16, 67-69.

FFT context."[18] Moreover, at that time the Commission stated that as it "gain[ed] further experience with the FFT program and review[ed] the data provided by NERC in its compliance and informational filings, [it] will consider and evaluate ways to improve the program" by "soliciting input from NERC, the Regional Entities, and industry when addressing such issues."[19] The Trade Associations encourage the Commission not to use a FOIA request to depart substantially from this policy. To the extent that the Commission is now considering a different approach, we ask that the Commission adhere to its prior commitment to invite these stakeholders to discuss the matter and avoid straying from the original approach in a response to the underlying FOIA request.

In a June 2013 FFT Order on Compliance related to implementation of the FFT and enhancements thereto, the Commission reiterated the general rule that "FFT informational filings must publicly identify the registered entity with a possible violation,"[20] but stated "[f]or FFTs involving the **CIP Reliability Standards, the Regional Entities would continue to redact the identity of the registered entities** involved in the issue and provide access to the non-public versions of these FFTs to NERC and FERC."[21] The Commission approved this compliance filing without modifying this aspect, designating information associated with CIP Reliability Standard violations as non-public information not subject to disclosure.[22] Importantly, the Commission emphasized the importance of protecting the identity of entities with CIP Standards violations:

> The Commission emphasizes that Regional Entities must continue to take precautions to protect non-public, confidential information and **redact any details** that could be used with publicly available information with respect to violations of the CIP Reliability Standards, such as the Regional Entities' audit schedule, **to identify the registered entity**. This is especially relevant in cases where the FFT is posted with ongoing mitigation activities because the registered entity may not have fully addressed any vulnerabilities resulting from the possible violation at the time of filing or posting.[23]

This approach to confidentiality with respect to the CIP Standards is settled, and a change to this policy requires a new proceeding with a broad opportunity for notice and comment to consider the implications of changing the existing Commission policy relied upon by NERC, Regional Entities, and registered entities.

The Trade Associations do not support a change in policy, especially in a response to a FOIA request. As noted above, publicizing the name of the registered entity with ongoing or repeated CIP or cybersecurity violations, even minor ones, may exacerbate cybersecurity risks and harm

---

[18] *Id.* at P 69.

[19] *Id.* at P 3 and n.2.

[20] *North American Electric Reliability Corporation*, 143 FERC ¶ 61,253, P 4 (2013) ("FFT Order on Compliance").

[21] *Id.* at P 19 (emphasis added).

[22] *Id.*

[23] *Id.* at P. 37 n.50 (emphasis added).

the public. For example, the Commission, while redacting certain information could, in theory, mitigate some risks, but such case-by-case consideration of confidentiality will vitiate any efficiency gains created through the FFT process. Moreover, subjecting utilities to subsequent disclosure under FOIA for violations could chill incentives for submitting nonpublic self-reports and undermine the existing enforcement and mitigation regime enshrined in the FFT process.[24] The broad request for disclosure of NOPs, which runs counter to existing FERC policy, is more appropriately considered in a public notice and comment proceeding, with the benefit of full stakeholder input and careful vetting of the ramifications.

Finally, it is worth noting that the registered entities have relied on NERC's and the Commission's existing approach to confidentiality, when engaging in good faith settlement negotiations and submitting self-reports. If FERC believes that it may now be appropriate to consider broad disclosure of sensitive information under FOIA that has historically been treated as confidential, any departure from the past practice should be applied on a prospective basis only, after public notice and an opportunity to comment on the proposed changes.

If the Commission decides to disclose any nonpublic information in responding to the FOIA Request, then the Commission must only provide information that will not risk jeopardizing the security of the Bulk-Power System.

To determine whether the information will jeopardize security, the Commission should provide the implicated UREs and NERC the opportunity to review the relevant records to determine the specific information that should be redacted to protect cybersecurity and the reliability of the Bulk-Power System. The Commission's FOIA process only provides parties five business days to respond, which is insufficient time to replicate the thoughtful decision-making processes provided by a rulemaking. For example, if FERC is considering disclosing a list identifying the registered entities that received an NOP, 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.

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 completely in order to protect public safety and national security as described above.

Alternatively, if the Commission believes that it should change its disclosure policy, then the Commission should do so in a full and open proceeding where all parties and interested actors

---

[24] Courts have recognized this concern about the government's ability to acquire information. The D.C. Circuit's test for the application of FOIA Exemption 4 asks whether disclosure of confidential information would "1) [. . .] impair the Government's ability to obtain necessary information in the future; or (2) [. . .] cause substantial harm to the competitive position of the person from whom the information was obtained. The test for confidentiality set forth in *National Parks* was subsequently adopted by nearly all of the other circuits, including the Ninth Circuit." *Dow Jones Co. v. F.E.R.C.*, 219 F.R.D. 167, 176–77 (C.D. Cal. 2003) (citing *National Parks and Conservation Ass'n v. Morton*, 498 F.2d 765 at 770 (D.C. Cir. 1974) ("*National Parks*")).

may participate and comment on the policy risks involved. Where the public and the nation is at risk from a proposed change in Commission policy, the public can only benefit if the Commission weighs and adjudicates on these issues in an open rulemaking proceeding. 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

Cc: Toyia.Johnson@ferc.gov, foiaceii@ferc.gov, edwin.kichline@nerc.net, Sonia.mendonca@nerc.net, james.danly@ferc.gov, david.morenoff@ferc.gov, joseph.mclelland@ferc.gov, dpatterson@publicpower.org, Randolph.Elliott@nreca.coop

Appendix B

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