UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	)	Docket Nos. NP10-130-000,
	)	NP10-131-000, NP10-134-000,
	)	NP10-135-000, NP10-136-000,
	)	NP10-137-000, NP10-138-000,
	)	NP10-139-000, NP10-140-000,
	)	NP10-159-000, NP10-160-000,
	)	NP11-1-000, NP11-2-000,
	)	NP11-3-000, NP11-4-000,
	)	NP11-5-000, NP11-21-000,
	)	NP11-22-000, NP11-47-000,
	)	NP11-56-000, NP11-59-000,
	)	NP11-63-000, NP11-64-000,
	)	NP11-70-000, NP11-72-000,
	)	NP11-76-000, NP11-79-000,
	)	NP11-81-000, NP11-102-000
	)	NP11-98-000; NP11-104-000,
	)	NP11-106-000, NP11-111-000,
	)	NP11-116-000, NP11-124-000,
	)	NP11-125-000, NP11-127-000,
	)	NP11-128-000, NP11-133-000,
	)	NP11-136-000, NP11-137-000,
	)	NP11-140-000, NP11-143-000,
	)	NP11-145-000, NP11-146-000,
	)	NP11-149-000, NP11-150-000,
	)	NP11-155-000, NP11-156-000,
	)	NP11-157-000, NP11-161-000,
	)	NP-162-000, NP11-166-000,
	)	NP-167-000, NP11-174-000,
	)	NP11-175-000, NP11-176-000,
	)	NP11-178-000, NP11-179-000,
	)	NP11-180-000, NP11-181-000,
	)	NP11-182-000, NP11-184-000,
	)	NP11-188-000, NP11-189-000,
	)	NP11-192-000, NP11-193-000,
	)	NP11-198-000, NP11-199-000,
	)	NP11-204-000, NP11-205-000,
	)	NP11-206-000, NP11-211-000,
	)	NP11-212-000, NP11-213-000
	)	NP11-218-000, NP11-223-000,
	)	NP11-225-000, NP11-226-000,
	)	NP11-229-000, NP11-230-000,

) NP11-233-000, NP11-234-000,
) NP11-237-000, NP11-243-000,
) NP11-247-000, NP11-248-000,
) NP11-249-000, NP11-250-000,
) NP11-251-000, NP11-253-000,
) NP11-261-000, NP11-262-000,
) NP11-263-000, NP11-264-000,
) NP11-266-000, NP11-269-000,
) NP11-270-000, RC11-6-000,
) NP12-1-000, NP12-2-000,
) RC12-1-000, NP12-3-000,
) NP12-4-000, NP12-5-000,
) RC12-2-000, NP12-10-000,
) NP12-9-000, RC12-6-000,
) NP12-11-000, NP12-12-000,
) RC12-7-000, NP12-16-000,
) NP12-17-000, NP12-18-000,
) RC12-8-000, NP12-20-000,
) NP12-22-000, RC12-10-000,
) NP12-25-000, NP12-26-000,
) RC12-11-000, NP12-27-000,
) NP12-29-000, RC12-12-000,
) NP12-36-000, RC12-13-000,
) NP12-37-000, NP12-38-000,
) NP12-40-000, RC12-14-000,
) NP12-43-000, NP12-44-000,
) RC12-15-000, NP12-45-000,
) NP12-46-000, NP12-47-000,
) RC12-16-000, NP13-1-000,
) NP13-4-000, NP13-5-000,
) RC13-1-000, NP13-6-000,
) RC13-2-000, NP13-11-000,
) NP13-12-000, NP13-16-000,
) NP13-17-000, NP13-18-000,
) NP13-19-000, RC13-3-000,
) NP13-22-000, NP13-23-000,
) RC13-5-000, NP13-24-000,
) NP13-27-000, RC13-6-000,
) NP13-30-000, NP13-28-000,
) NP13-29-000, NP13-32-000,
) NP13-33-000, RC13-8-000,
) NP13-34-000, NP13-38-000,
) NP13-39-000, RC13-9-000,
) NP13-41-000, RC13-10-000,
) NP13-45-000, NP13-46-000,
) NP13-47-000, NP13-51-000,

)	NP13-55-000, NP13-57-000,
)	NP14-4-000, NP14-5-000,
)	NP14-6-000, NP14-14-000,
)	NP14-16-000, NP14-17-000,
)	NP14-18-000, NP14-19-000,
)	NP14-20-000, NP14-22-000,
)	NP14-21-000, NP14-23-000,
)	NP14-24-000, NP14-25-000,
)	NP14-26-000, NP14-29-000,
)	NP14-30-000, and
)	NP19-4-000

MOTION TO INTERVENE AND PROTEST OF THE AMERICAN PUBLIC POWER ASSOCIATION, THE EDISON ELECTRIC INSTITUTE, AND THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

Pursuant to the Federal Energy Regulatory Commission's ("FERC" or "Commission") rule concerning the Enforcement of Reliability Standards, 18 C.F.R. § 39.7 (2018), the American Public Power Association ("APPA"), the Edison Electric Institute ("EEI"), and the National Rural Electric Cooperative Association ("NRECA"), (collectively, the "Trade Associations") respectively submit, on behalf of our members subject to the Notices of Penalty filed by the North American Electric Reliability Corporation ("NERC") in the above-captioned dockets ("Dockets"), this Motion to Intervene and Protest ("Motion") in response to other motions filed in the Dockets.

The genesis of each of the above-referenced Dockets was the filing of a Notice of Penalty by NERC for the Commission's approval. However, the other motions subsequently filed in the Dockets inappropriately seek the release of information redacted by NERC from the public versions of the Notices of Penalty. NERC has correctly redacted this information because it is

protected from disclosure under the Commission's Enforcement of Reliability Standards rule[1] and/or is Critical Energy/Electric Infrastructure Information ("CEII") protected by statute.[2]

The Dockets each relate to specific violations of the NERC Critical Infrastructure Protection Standards ("CIP Standards") that are mandatory cyber and physical security requirements designed to protect the most critical assets and systems of the bulk-power system against cyber and physical attacks. Due to the importance of the security information associated with the CIP Standards, the Trade Associations are compelled to respond and protest the motions filed in the Dockets. In addition, the Trade Associations can raise objections in response to the other motions that our members subject to these Notices of Penalty may not be in a position to make because they cannot respond in a public filing without identifying themselves.

The Commission should be vigilant in its decisions regarding the protection and treatment of CEII, the removal of CEII designations, and the release of information related to implementation of, compliance with, and enforcement of the CIP Standards. The growing sophistication and frequency of attacks against critical infrastructure necessitates such vigilance to ensure that information that could be used by attackers to endanger the security and reliability of the bulk-power system is protected. The Trade Associations recommend that the Commission not act on the information requests contained in the other motions in the Dockets, but instead initiate a rulemaking to allow all stakeholders an opportunity for notice and comment on these

[1] 18 C.F.R. § 39.7.

[2] The Commission's CEII regulation includes critical electric infrastructure information and critical energy infrastructure information. 18 C.F.R. § 388.113. Critical electric infrastructure information is related to a system or asset of the bulk-power system that if incapacitated or destroyed would negatively affect national security, economic security, and/or public health or safety. *Id*. at (c). Critical energy infrastructure information is information on a vulnerability or detailed design information on systems or assets that relate to the bulk-power system and could be useful to a person planning an attack on that system or asset. *Id.* The Commission's rules for CEII have been expanded in accordance with the Fixing America's Surface Transportation Act ("FAST Act") to provide stronger information protection. *Regulations, Implementing FAST Act Section 61003 – Critical Infrastructure Security and Amending Critical Energy Information*, Order No. 833, 157 FERC ¶ 61,123 (November 17, 2016) ("Order 833").

issues. In particular, the Commission should not change its procedures and policies related to disclosure of information related to the CIP Standards without such opportunity for notice and comment.

I. MOTION TO INTERVENE

Pursuant to the Commission's rule concerning the Enforcement of Reliability Standards, 18 C.F.R. § 39.7, the Trade Associations submit the following in support of this Motion. Members of the Trade Associations are subject to the mandatory Reliability Standards developed by NERC and enforced by the Commission and NERC, including the CIP Standards, compliance with which is addressed in the Dockets.

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 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.

NRECA is the national service organization for the nation's member-owned, not-for-profit electric cooperatives. Nearly 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 13% of the nation's electric customers, while accounting for approximately 12% 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.

The Trade Associations provide a broad perspective on the issues raised in the Dockets that cannot be adequately represented by any other party. In particular, the parties subject to the penalties may not be able to file responsive pleadings on their own behalf in the Dockets if doing so would identify them as a party subject to a penalty, which is the very information the other intervenors seek. Granting this Motion will not delay the proceeding or unduly prejudice any party.[3] The Trade Associations do not seek Commission review of any of the Notice of Penalties in the Dockets, many of which have already closed by operation of law pursuant to 18 C.F.R. §39.7(e)(2). Rather, the Trade Associations seek to participate in these proceedings for the limited purpose of protesting other efforts to intervene and suggesting that the Commission initiate a rulemaking to address the requests for information. If the Commission grants any of the Motions to Intervene in any of the Dockets, then the Trade Associations respectfully request that the Commission also grant this Motion to Intervene and allow the Trade Associations to become a party to the proceeding(s).

[3] *See*, *e.g.*, 18 C.F.R. § 385.214(d) (2007) (requirements for motion for late intervention); *Consolidated Gas Supply Corp.*, 20 FERC ¶ 61,305, at 61,599 (1992) (factors considered by Commission in determining whether good cause exists to permit late intervention).

II. NOTICES AND COMMUNICATIONS

All communications and correspondence with respect to this Motion should be served upon the following individuals who should be included on the official service lists compiled by the Secretary of the Commission in these proceedings:[4]

Delia D. Patterson
SVP Advocacy & Communications and General Counsel
American Public Power Association
2451 Crystal Dr., Suite 1000
Arlington, VA 22202
Phone: 202-467-2900
Email: dpatterson@publicpower.org

Emily Sanford Fisher
General Counsel and Corporate Secretary
Edison Electric Institute
701 Pennsylvania Ave, N.W.
Washington, D.C. 20004
Phone: 202-508-5000
Email: efisher@eei.org

Randolph Elliott
Senior Director, Regulatory Counsel
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
Phone: 703-907-6818
Email: Randolph.Elliott@nreca.coop

III. COMMENTS

On February 19, 2019 Michael Mabee filed a Motion to Intervene in 192 Notice of Penalty dockets dating from July 2010 to January 2014 ("Motion 1"). In Motion 1, he argues that the CEII designations for these penalties have expired and requests that the Commission release all of the documents related to these penalties that are not already public. On February

[4] The Trade Associations request waiver of 18 C.F.R. § 385.203(b)(3) to permit more than two persons to be added to the service list.

21, 2019, Mr. Mabee filed another Motion to Intervene under Docket No. NP19-4-000 ("Motion 2") (Motion 1 and Motion 2 collectively referred to as "Mabee Motions"), which requested that the Commission review the Notice of Penalty and release the entity name—which is redacted from the publicly-available version of the Notice of Penalty—and unredacted versions of the Notice of Penalty and related settlement agreements between NERC and the unnamed entity. In both Mabee Motions, Mr. Mabee asserts—directly and indirectly—that there has been a lack of public transparency with regard to these penalties. In addition, other private citizens,[5] Public Citizen,[6] and the Foundation for Resilient Societies[7] filed similar motions to intervene in Docket No. NP19-4-000; however, Public Citizen only requested the entity name for that Docket.

The Commission should not act on these motions because intervention is not a legally available option for these parties. The Commission also should not release the requested information in any of these Dockets because the motions made by Mr. Mabee and the others are not appropriate mechanisms for information requests. Freedom of Information Act ("FOIA") requests are the appropriate mechanism to request such information. However, the information requested relates to the CIP Standards that has been appropriately redacted by NERC because it is CEII and/or is protected under the Commission's Enforcement of the Reliability Standards rule[8] and therefore cannot be disclosed. Moreover, as described below, public release of this information could have a negative impact on the reliability and security of the bulk-power system and therefore the Commission should not disclose such information in response to the motions or a FOIA request.

[5] For example, two motions were filed by Dale Rowley filed on February 26 and March 23; Karen Testerman filed a motion on March 25; and Fred A. Reitman filed a motion on March 27, 2019.

[6] February 19, 2019.

[7] March 26, 2019.

[8] 18 C.F.R. §39.7.

The Trade Associations encourage the Commission to be transparent to the public and vigilant in making decisions regarding release of information related the CIP Standards. In making such decisions, the Commission must balance transparency and national security. To achieve the appropriate balance, the Trade Associations recommend that the Commission seek broader input from all stakeholders through a rulemaking before changing the precedent set in and maintained since 2010 related to disclosure of information related to the CIP Standards.[9]

A. The Commission should not act on the motions in the Dockets because intervention is not a legally available option for the filers and the Notice of Penalty dockets are not an appropriate place for either information requests or releases.

The Commission's rule concerning the Enforcement of Reliability Standards enables a "user, owner or operator" that is subject to a penalty due to a Reliability Standard violation to file an application for the Commission to review the penalty within 30 days from when NERC files the Notice of Penalty with the Commission.[10] None of the filers of the motions in these Dockets are a "user, owner or operator" subject to a penalty and therefore the rule does not afford them the opportunity to seek review of the penalties. Also, all of the dockets listed in Motion 1 have already been "affirmed by operation of law."[11]

The only procedural avenue for a party—who is not subject to the penalty—to intervene is within 20 days after the party subject to the penalty has filed an application for the Commission to review the penalty. Regarding Docket No. NP19-4-000, no application for review has been filed and the Commission has not given public notice of whether it will review

[9] Mr. Mabee also filed a "Petition for Rulemaking" with the Commission. However, his petition appears on the Commission's eLibrary at accession number 20190205-5150 as an undocketed filing that has not been noticed for public comment. As a result, the Trade Associations cannot file a response pleading.

[10] 18 C.F.R. § 39.7(e)(1).

[11] *Id.* at § 39.7(e)(2).

the Notice of Penalty on its own motion. Therefore there is no application for review upon which a party could seek to intervene or comment.[12] Finally, even if the Commission were to give public notice that it will review on its own motion the violations in Docket No. NP19-4-000, due to the CEII contained within the Notice of Penalty, the Commission should conduct such a review in a non-public proceeding.[13] As a result, these Dockets are not available to entities generally seeking either to intervene or request the release of information, let alone information designated as CEII.

Also, the Commission's regulations regarding the enforcement of the Reliability Standards should not be used to compel the Commission to review CEII designations and release information. No part of 18 C.F.R. § 39 establishes such a process. If the Commission grants the motions in the Dockets, it will: (1) arbitrarily and capriciously create new vehicles through which entities can request information and the Commission can disclose information outside of its existing procedures for information requests and disclosure;[14] (2) set new precedent that would enable anyone to intervene in Notice of Penalty dockets, a right which is currently limited by the Commission's regulations to permit requests for review of the penalty only by the party subject to the penalty or the Commission on its own motion;[15] and (3) undermine the

[12] *Id.* at § 39.7(e)(4).

[13] On February 22, the Commission issued a notice to extend its time period for consideration on whether to review on its own motion the Notice of Penalty violations in Docket No. NP19-4-000 until March 29, 2019, but has not yet made a determination as to whether it will review on its own motion. NERC has redacted CEII from this Notice of Penalty and therefore if the Commission decides on its own motion to review the violations, then the Commission will likely—and appropriately—determine that a non-public proceeding is necessary and lawful. As a result, the public, including the Trade Associations, will not be notified and not be allowed to participate. 18 C.F.R. §39.7(e)(7) (2018).

[14] A court will uphold an agency decision under the arbitrary and capricious standard "if the agency has 'examine[d] the relevant [considerations] and articulate[d] a satisfactory explanation for its action[,] including a rational connection between the facts found and the choice made.'" *FERC v. Elec. Power Supply Ass'n*, 136 S. Ct. 760, 782(2016) (quoting *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983)).

[15] *Id.* at (e)(4)-(7).

Commission's own "long-standing procedures" for the administration of information requests,[16] which were recently revised as directed by Congress in the FAST Act to carefully balance public interest, national security, confidentiality, and due process.[17]

Accordingly, the appropriate mechanism to seek Commission review and disclosure of information designated as CEII is through a FOIA or CEII request, which is a mechanism that has also been pursued by Mr. Mabee. The Commission already has begun processing the 242 FOIA requests filed by Mr. Mabee seeking the release of similar information. Mr. Mabee has submitted these FOIA requests with the stated intent of making any released information public on his blog, where he also advertises a book he has written for purchase. The Trade Associations also oppose the release of information in response to these FOIA requests because such a release is not in the public interest as it could be used to negatively impact the reliability and security of the bulk-power system.[18]

The Trade Associations agree that public transparency is important, and it is clear from the motions in the Dockets that the filers are concerned about the security of the bulk-power system. Nonetheless, these motions do not properly reflect the unique regulatory process governing the CIP Standards, the content of the Notice of Penalties and settlement agreements related to the CIP Standards, and/or the security implications for public disclosure related to CIP

[16] Order No. 833-A a P 7; *see also* 18 C.F.R. § 388.108 (Commission regulations for FOIA requests). In Order No. 833, the Commission noted that its current CEII process "is designed to limit the distribution of sensitive infrastructure information to those individuals with a need to know in order to avoid having sensitive information fall into the hands of those who may use it to attack the Nation's infrastructure." Order No. 833 at P 4.

[17] Fixing America's Surface Transportation Act, Pub. L. No. 114-94, section 61,003, 129 Stat. 1312, 1773-1779 (2015) (codified at 16 U.S.C. 824o-1); Order 833 (Final Rule implementing FAST Act provisions regarding the designation, protection, and sharing of CEII and revising existing CEII regulations). The Commission's regulations governing requests for CEII require the balancing of "the requester's need for the information against the sensitivity of the information." 18 C.F.R. § 388.113(g)(5)(iii).

[18] Appendix 1 and 2 include our previous responses to the Submitter's Rights Letters for FOIA Nos. FY19-19 and FY19-030.

Standards violations. For example, the CIP Standards do not protect nuclear generation facilities; there are separate requirements developed and enforced by the Nuclear Regulatory Commission that are responsible for nuclear facilities.[19] In addition, penalties are given when a Registered Entity is found noncompliant with a requirement of a CIP Standard and are not an indicator that a system has been infiltrated.[20]

Also, the filers appear to rely on media reports as their source of information and do not appear to have engaged in any of NERC's public processes (e.g., standards development). The public—including the filers—can directly participate in the standards development and other processes at NERC. In addition, once the Commission approves the CIP Standards that are developed by NERC in this public process, they are mandatory and enforceable regulatory requirements. Registered Entities cannot pick and choose the requirements with which they want to comply. They must comply with all applicable requirements and their compliance therewith is audited by NERC, Regional Entities, and/or FERC. Non-compliance—even self-reported non-compliance—can result in financial penalties in addition to further mitigation requirements. The fact that the penalties and associated mitigation measures are negotiated and ultimately settled does not in any way render them toothless, as filers suggest. Rather, the collaborative nature of the Reliability Standards enforcement regime is a critical aspect of the Reliability Standards to facilitate the objective—to provide for the reliability and security of the bulk-power system. The high proportion of self-reports described above demonstrates the value

[19] In Docket No. NP10-4-000 (Motion 2), Mr. Mabee expressed concern with blackouts resulting in the release of radioactive contaminants from nuclear plants. Michael Mabee, Motion to Intervene, Docket No. NP19-4-000 (Feb. 21, 2019).

[20] In Dale Rowly's March 23 motion, the request for the entity name in Docket No. NP19-4-000 is tied to whether the Commission finds a Registered Entity system to have been infiltrated and that such infiltration is serious enough to require a penalty, then these entities should be identified. Dale D. Rowley, Motion to Intervene, Docket No. NP19-4-000 (Mar. 23, 2019). The Trade Associations are unaware of any findings by the Commission related to system infiltration.

and effectiveness of collaborative efforts to operate the bulk-power system in a reliable, secure manner.

B. Release of additional Notice of Penalty information could negatively impact the reliability and security of the bulk-power system.

In accordance with the implementation plans for the CIP Standards, NERC began filing penalties at the Commission for violations of the CIP Standards in July 2010. The CIP Standards include physical and cybersecurity regulatory requirements designed to protect Registered Entity cyber systems that "if rendered unavailable, degraded, or misused" may have an adverse impact on a Registered Entity facility, system, or equipment that could affect the reliable operation of the bulk-power system.[21] The CIP Standards are enforced by FERC, NERC, and the Regional Entities. NERC files a public and non-public version of each Notice of Penalty with the Commission as an outcome of this enforcement activity. The public version does not include sensitive information, including privileged information and CEII. Recently, starting with Docket No. NP19-4-000, NERC began filing a full, redacted version[22] and a full, unredacted version of the Notice of Penalty with the Commission rather than filing separate public and non-public versions. Only the redacted version of the Notice of Penalty is publicly posted.

---

[21] A Bulk-Electric System Cyber Asset is defined by NERC as:

> [a] Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

NERC Glossary of Terms.

[22] The full, redacted version has CEII blacked out, whereas the previously filed public versions only included non-CEII information without black-out markings. The full, redacted version gives the public a better visual sense of how much information is redacted.

The Trade Associations understand that in 2010 NERC and the Commission intentionally chose to post only the public versions of the Notices of Penalty without the names of the entities to address security concerns because the names, when combined with information on the violations and penalties, were considered CEII. In addition to the entity names, details on cybersecurity vulnerabilities and mitigation measures that can be used by an attacker to determine which entity to target; what device or system to target; and how to target that entity, device, or system were also intentionally left out of the public versions. Disclosing this information to the public will not only be useful to those who seek to attack the bulk-power system, but will also have a negative impact on the effectiveness of the Commission's compliance and enforcement activity.

1. Public disclosure of new details on CIP Standards violations and penalties will be useful to those seeking to attack the bulk-power system.

The cyber and physical security requirements of the CIP Standards have significantly evolved since 2010. Meanwhile, the array and capabilities of hostile forces seeking to attack the U.S. electric grid and destabilize the nation have increased in size and sophistication. In the past year, the FBI and Department of Homeland Security publicly revealed that a foreign nation-state engaged in a prolonged, "multi-stage intrusion campaign" against U.S. utilities.[23] Also, the Department of Justice ("DOJ") recently indicted foreign hackers who successfully penetrated hundreds of U.S. institutions. In releasing the indictment, the DOJ specifically called out the

[23] 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.

grave risk posed by malicious actors targeting the U.S. electric sector, including the Commission itself, for access to sensitive information.[24]

The information requested in the Dockets—and the FOIA requests mentioned above—is exactly this type of sensitive information. Making this information public would assist people seeking to attack U.S. electric infrastructure. Even information such as revealing the name of an entity involved in a remediated Notice of Penalty can result in unintended consequences. For example, an entity name coupled with details about past violations—including system or company information—provides not only a target, but also useful information for an attacker in developing a phishing campaign designed to target that entity to gain security credentials and system access. Attackers are creative and endlessly innovative; they can use new information in a variety of ways, particularly if they have already begun "mapping" our electric system.[25]

In addition, Registered Entities 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 based on information culled from the public versions of the Notice of Penalties—especially when such information is coupled with the entity's name and other publicly available information. The Trade Associations recognize that public access to information is important, and appreciates the goals of public transparency, but the line must be drawn in favor of protecting sensitive information where a requested disclosure could have a negative impact on reliability and security of the nation's bulk-power system.

[24] 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

[25] Daniel R. Coats, Statement for the Record Worldwide Threat Assessment of the US Intelligence Community (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

2. Changing disclosure precedent will impact the effectiveness of the Commission's compliance and enforcement of the CIP Standards.

The Commission also should consider the adverse impact of releasing information—previously not disclosed to the public—on its compliance and enforcement regime. The confidentiality[26] associated with compliance and enforcement of the CIP Standards allows for lessons learned between the regulators[27] and Registered Entities to achieve the goals of the CIP Standards—to provide for the security and reliability of the bulk-power system.

For example, NERC and the Regional Entities rely heavily on voluntary self-reports of CIP Standards violations by Registered Entities. During the February NERC Board Meetings, NERC staff reported that **76.2 percent** of the violations were identified by self-reports and only 19.1 percent were identified by audit findings. This is evidenced in NP19-4-000, where 111 out of 127 violations were self-reported (87.4 percent) and only 16 (12.6 percent) were found in audits. These voluntary self-reports contain operational and technical data that are intended to inform the relevant compliance enforcement authority on the nature of a possible violation to support the resolution of the identified issue. If the Commission begins releasing entity names in addition to the information already made public in the posted Notices of Penalty, then Registered Entities may re-evaluate whether they will continue to self-report security information knowing that providing such information to their regulators may be disclosed to the public, including to people seeking to attack their systems.

In addition, Registered Entities also may re-evaluate what information is included in their mitigation plans. Providing details of their security measures in these plans and through other

[26] Through privileged information (18 C.F.R. §388.112), CEII (18 C.F.R. §388.113), and 18 C.F.R. §39.7 protections.

[27] FERC, NERC, and the Regional Entities.

interactions with the Commission becomes a security risk if the Commission determines that a requester needs this information. This will make entities reluctant to share information with the Commission and have a chilling effect on the quality of the information communicated to FERC, NERC, and the Regional Entities. Lessening the quality of information shared with regulators will mute the quality of lessons learned by FERC, NERC, and stakeholders in the compliance and enforcement process. To minimize these impacts, the Commission should avoid creating disclosure regimes that undermine the very goals the CIP Standards seek to achieve—to provide for the security and reliability of the bulk-power system.[28]

The CIP Standards are different than other regulatory schemes. Although in other regulatory schemes "shaming" violators may serve as a deterrent to noncompliant behavior or as a way to modify consumer behavior, naming the Registered Entities who have instances of CIP Standards noncompliance would not accomplish any measurable goal despite the vague public benefits claimed by the other intervenor filers. First, the CIP Standards requirements are meant to protect Registered Entity systems that could have an impact on the bulk-power system from cyber and physical attacks, including attacks by nation state threat actors. Registered Entities are the potential victims of these attacks. Registered Entities already are incentivized to implement effective cyber security controls to ensure the reliability of their own operations and the CIP Standards were designed to help entities protect their assets and the bulk-power system from cyber and physical attacks. It also is not uncommon for Registered Entities to implement

[28] 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*")).

security measures that go above and beyond the requirements in the CIP Standards. The financial penalties imposed on Registered Entities for CIP Standards violations serve to punish the potential victims (i.e., Registered Entities)—as evidenced by the increasing size of such penalties. Although Registered Entities that have CIP Standards violations are subject to financial penalties, the standards were not intended to function solely as a punitive regulatory mechanism. The Commission and the public should consider whether further "shaming" of Registered Entities by publicly naming them is in the best interests of a regulator trying to improve national security and consistent with the goals of the CIP Standards.

Second, the impact on public safety and on consumer behavior is less direct for the enforcement regimes for the CIP Standards. When a Registered Entity is in violation of a requirement of the CIP Standards, the impact to the public is less clear compared to food recalls and airplane crashes. For food recalls, the public needs to know which products to return and members of the public are on the planes that crash. The public may not even be impacted by a CIP Standard violation, they are not a part of the violation, and cannot act to secure the Registered Entity's system; only the owner or operator of the impacted system can take such actions. However, the disclosure of details on which entity and what actions that Registered Entity takes to mitigate noncompliance with a CIP requirement would be useful to the very people seeking to disrupt the reliability of the bulk-power system.

In addition, much information regarding non-compliance with the CIP Standards is already made publicly available in the public versions of the Notices of Penalty. This information includes the region in which the Registered Entity is located, the standard violated, the nature of the violation, the reliability risk created by the violation, and the steps taken to

mitigate the violation. In addition to providing public transparency, this information provides critical guidance to the industry and is regularly reviewed by compliance personnel.

C. The Commission should initiate a rulemaking to evaluate transparency and security concerns before changing precedent on its disclosure of information related to CIP Standards violations.

The Commission has recently begun establishing criteria to evaluate such disclosures on a case-by-case basis.[29] However, the Commission appears to be developing and evaluating these criteria without input from stakeholders, including Registered Entities, NERC, and the public.[30] To support transparency to the public and to Registered Entities, the Trade Associations encourage the Commission to institute a public rulemaking proceeding to allow stakeholders to weigh in on the criteria and the Commission's procedures on what information can and should be disclosed and how to best evaluate potential disclosure of this information.

Transparency issues or concerns regarding CIP Standards violations should be evaluated through a public process that allows for the robust exchange of ideas, comments, concerns, and alternatives. The Commission should initiate a rulemaking process to clearly identify the criteria for disclosing information concerning CIP Standards violations. A rulemaking will allow the public to provide input to the Commission regarding the information it wants with regard to CIP Standards violations and demonstrate the benefits of making this information public. A rulemaking also will allow a broader range of Registered Entities to explain why some

[29] A Notice of Intent to Release under Docket No. FOIA FY19-19 issued on February 28, 2019 by the Commission applies seven factors for a case-by-case assessment: "the nature of the CIP violation; whether mitigation is complete; the content of the public and non-public versions of the Notice of Penalty; the extent to which the disclosure of the pertinent URE identity would be useful to someone seeking to cause harm; whether an audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public Notice of Penalty." These factors were also applied in a Notice of Intent to Release under Docket No. FOIA FY19-30 issued on March 20, 2019 by the Commission.

[30] In the original Submitter's Rights Letter for FOIA FY19-19, these seven criteria were not mentioned and therefore NERC nor the UREs affected did not have a chance to weigh in on each of these criteria in opposing the release of information.

information should not be made public without concerns about disclosing their name as associated with a particular Docket. The Commission could then use the information gleaned through the rulemaking process to revise its procedures on information disclosure.[31]

The Trade Associations understand that the Commission currently is headed down a path of releasing entity names related to more administrative CIP Standard violations and is considering further release of technical violations in response to the FOIA requests. While the release of administrative violations will identify which entities made paperwork mistakes, it will not help the public to understand what is being done by Registered Entities, NERC, and FERC to secure the bulk-power system. Even the release of entity names with more technical violations will not achieve this goal, as many of the details are contained within the full, unredacted Notice of Penalties and settlement agreements, which should not be made public. The Trade Associations encourage the Commission to enhance transparency and improve its processes to support bulk-power system security in a more comprehensive manner. However, we are concerned that without a robust stakeholder process to address how to balance these interests, the resulting information disclosures could have unintended consequences for the bulk-power system.

[31] Including 18 C.F.R. §§ 39.7 and 388.

IV. CONCLUSION

The Trade Associations appreciate being able to submit comments on this important issue and respectfully requests that the Commission consider instituting a rulemaking proceeding to weigh improvements to its regulations to improve both public transparency and security of the bulk-power system.

Respectfully submitted,

/s/ Delia D. Patterson
SVP Advocacy & Communications and General Counsel
American Public Power Association
2451 Crystal Dr., Suite 1000
Arlington, VA 22202
Phone: 202-467-2900
Email: dpatterson@publicpower.org

/s/ Emily Sanford Fisher
General Counsel and Corporate Secretary
Edison Electric Institute
701 Pennsylvania Ave, N.W.
Washington, D.C. 20004
Phone: 202-508-5000
Email: efisher@eei.org

/s/ Randolph Elliott
Senior Director, Regulatory Counsel
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
Phone: 703-907-6818
Email: Randolph.Elliott@nreca.coop

March 28, 2019

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document upon each person designated on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 28th day of March, 2019.

/s/ Megan Vetula
Associate General Counsel, Energy Regulation
Edison Electric Institute
701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
Phone: (202) 508-5000
Email: mvetula@eei.org

APPENDIX 1

Document Accession #: 20190328-5298 Filed Date: 03/28/2019

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-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 2

Document Accession #: 20190328-5298 Filed Date: 03/28/2019

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

Document Content(s)