UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL MABEE, Plaintiff, v. FEDERAL ENERGY REGULATORY COMMISSION, Defendant.	Civil Action No. 19-3448 (ACR)

DEFENDANT'S CORRECTED MOTION FOR SUMMARY JUDGMENT

Defendant, Federal Energy Regulatory Commission ("FERC"), by and through undersigned counsel, respectfully moves for summary judgment in its favor pursuant to Federal Rule of Civil Procedure 56.[1] In sum, there exists no genuine issue of material fact and FERC is entitled to judgment as a matter of law in this Freedom of Information Act ("FOIA") case. In support of this Motion, FERC refers the Court to the accompanying memorandum, statement of material facts, declaration of Barry W. Kuehnle, and the attached exhibits. A proposed order is also enclosed herewith.

This case involves three FOIA requests by Plaintiff to FERC, dated December 18, 2018, January 12, 2019, and August 3, 2019, for documents revealing the names or identities of various Unidentified Registered Entities. FERC has produced all responsive, non-exempt material to Plaintiff. Accordingly, there are no issues of material fact in genuine dispute, and any information not provided was properly withheld pursuant to an exemption under FOIA.

[1] Defendant timely filed its Motion for Summary Judgment yesterday (ECF No. 55), but undersigned counsel subsequently realized that the filed brief inadvertently lacked a table of contents and table of authorities. Defendant now files, with Plaintiff's consent, a corrected brief that differs only in the inclusion of those tables.

Dated: March 5, 2024
Washington, DC

Respectfully submitted,

MATTHEW M. GRAVES
D.C. Bar No. #481052
United States Attorney

BRIAN P. HUDAK
Chief, Civil Division

By: */s/ Kartik N. Venguswamy*
KARTIK N. VENGUSWAMY
D.C. Bar No. #983326
Assistant United States Attorney
601 D Street, NW
Washington, D.C. 20530
Tel: (202) 252-1790
kartik.venguswamy@usdoj.gov

Attorneys for the United States of America

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL MABEE,

Plaintiff,

v.

FEDERAL ENERGY REGULATORY COMMISSION,

Defendant.

Civil Action No. 19-3448 (ACR)

DEFENDANT'S MEMORANDUM IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations

By and through its undersigned counsel, Defendant the Federal Energy Regulatory Commission ("FERC" or the "Agency") respectfully submits this memorandum of points and authorities in support of the Agency's motion for summary judgment. In sum, there exists no genuine issue of material fact that precludes judgment in the Agency's favor as a matter of law in this Freedom of Information Act, 5 U.S.C. § 552 ("FOIA") case.

As set forth below, and pursuant to Federal Rule of Civil Procedure ("Rule") 56, the Agency should be granted summary judgment because no genuine issue of material fact exists, and therefore the Agency is entitled to judgment as a matter of law.

PRELIMINARY STATEMENT

Plaintiff, Michael Mabee, commenced this FOIA action on November 15, 2019. *See generally* Compl. (ECF No. 1). Under FOIA, Plaintiff made requests to FERC, dated December 18, 2018, January 12, 2019, and August 3, 2019, for documents revealing the names or identities of various Unidentified Registered Entities.

FERC has produced all responsive, non-exempt material to Plaintiff. There are no issues of material fact in genuine dispute. As explained herein and in the attachments hereto, any information not provided was properly withheld pursuant to an exemption under FOIA.

INTRODUCTION

This case arises from Plaintiff's three FOIA requests directed to the Agency seeking the previously undisclosed names of utilities throughout the United States addressed within public Notices of Penalty[2] issued by the North American Electric Reliability Corporation ("Reliability

[2] There are three variations of a penalty filing: a "Notice of Penalty," a "Spreadsheet Notice of Penalty," and a "Find, Fix, and Track Report." The latter two generally address, within a single document, numerous entities and associated violations. "A Notice of Penalty" generally addresses one Entity and certain related violations. For purposes of this brief, all the foregoing variations of penalty filings will be referred to collectively by the term "Notice of Penalty."

Corporation") in connection with audits of Critical Infrastructure Protection Reliability Standards (the "Reliability Standards"). The audits at issue relate to violations by various utilities—referred to in the public Notices of Penalty as one or more Unidentified Registered Entities ("Entities")—of cybersecurity-related reliability standards designed to protect the nation's bulk electric system.

Plaintiff's FOIA requests seek the names of the Entities associated with over 253 Notice of Penalty public administrative proceedings identified by separate FERC docket numbers. While there are 253 Notice of Penalty dockets at issue in this case, there are approximately 1,500 Entities that are addressed therein. *See supra* n.1.

In connection with Plaintiff's requests, FERC has undertaken an individualized assessment of each Entity addressed in each docket and the potential risks associated with the disclosure of their names. Based on these assessments, FERC staff has concluded that most Entity identities should be withheld pursuant to FOIA Exemptions 3 and 7(F). FERC staff did, however, release some Entity information after consideration of the following factors: the nature of the information contained in the publicly available version[3] of the Notice of Penalty; the nature of the Reliability Standard violation, including whether there is a Technical Feasibility Exception involved that does not allow an Entity to fully meet the Critical Infrastructure Protection standards; whether vendor-related information is contained in the Notices of Penalty; whether mitigation is complete; the extent to which the disclosure of the identity of the Entity and other information would be useful to someone seeking to cause harm; whether a successful audit has occurred since the violation; whether the violation was administrative or technical in nature; and the length of time that has

[3] The Reliability Corporation files Notices of Penalty in both non-publicly available versions, which contain information designated as Critical Electric Infrastructure Information pursuant to 16 U.S.C. § 824o-1(a)(3), as well as public Notices of Penalty, in which such information has been redacted. *See* Kuehnle Decl. ¶ 10.

elapsed since the filing of the public Notice of Penalty. Kuehnle Decl. ¶ 14, attached hereto as Exhibit 1. Plaintiff does not challenge any particular determination, nor does he specifically refute any of FERC's individualized assessments of Entities. Instead, he asserts that, without limitation, the identities of all Entities should be disclosed to him. Caselaw establishes, however, that such a release to anyone, including plaintiff, would be a release to all, including potential bad actors.

In instances in which the Agency's assessment concluded that the risk of disclosing the identity of an Entity created a material risk to the bulk electric system, FERC applied Exemptions 3 and 7(F) and determined that each exemption formed a basis to withhold the identities. With respect to Exemption 3, FERC determined that the identities of certain Entities constituted "Critical Electric/Energy Infrastructure Information," as defined in the Fixing America's Surface Transportation Act ("FAST Act") and FERC-promulgated regulations. *See* 16 U.S.C. § 824o-1(d)(1)(A) ("critical electric infrastructure information—(A) shall be exempt from disclosure under section 552(b)(3) of title 5[.]"). With respect to Exemption 7(F), FERC determined that Entity identities, in concert with the publicly available Notices of Penalty, constituted "records or information compiled for law enforcement purposes, [the disclosure of which], could reasonably be expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(F).[4] As discussed in more detail below, because the Agency's determinations are consistent with the application of the foregoing FOIA exemptions, summary judgment in its favor is appropriate.

[4] Pursuant to this Court's order, FERC also submitted ten exemplar Notices of Penalty for *in camera* review on January 31, 2024, to let this Court see for itself the importance of withholding the information that FERC redacted. *See* ECF No. 53.

FACTUAL BACKGROUND

A. Security of the Nation's Electric Grid.

On July 20, 2006, FERC certified the Reliability Corporation pursuant to authority delegated under section 215 of the Federal Power Act as the nation's designated Electric Reliability Organization. 116 FERC ¶ 61,062. Upon this certification, the Reliability Corporation became responsible for, among other things, the development and enforcement of reliability standards designed to, as the name implies, maintain the reliability of the United States' electric grid. *Id.* Such reliability standards include requirements associated with ensuring the physical security of electric infrastructure as well as requirements associated with ensuring the integrity of electric cyber security infrastructure. *Id.*; Kuehnle Decl. ¶ 8. By way of example, the reliability standards at issue here—the Critical Infrastructure Protection Reliability Standards—address matters such as background checks for employees with access to critical cyber assets, assuring that electric utilities and other industry stakeholders timely install security patches to protect software, and adequately training of electric utility staff on cyber security response measures. Kuehnle Decl. ¶ 8.

The Reliability Corporation, together with its six "Regional Entities" located throughout the United States and Canada, conducts audits and other assessments regarding electric utility companies' compliance with the Reliability Standards. *Id.* ¶ 9. Other assessments include, by way of example, self-certifications, spot-checks, compliance investigations, self-reporting, and self-logging. These assessment tools, as well as other aspects of other aspects of the Reliability Corporation's Compliance Monitoring and Enforcement Program are set forth in Appendix 4C of the Reliability Corporation's Rules of Procedures found at https://www.nerc.com/AboutNERC/RulesOfProcedure/NERC_ROP_With_Appendices.pdf. Part of the enforcement actions for the non-compliance are mitigation plans and, where appropriate, monetary penalties. *Id.*

B. The Reliability Corporation's Notices of Penalty.

Upon completion of an audit, the Reliability Corporation and the Regional Entities may refer audit findings to their enforcement staff as potential violations of the Reliability Standards. *Id.* ¶ 10.

Upon finding of a violation and determination of a monetary penalty—or, more often settlement with the alleged violator—the Reliability Corporation then files a "Notice of Penalty" with FERC. *Id.*; *see also* 16 U.S.C. § 824o(e)(2); 18 C.F.R. § 38.7(e). Section 215(e)(2) of the Federal Power Act provides that a penalty submitted by the Reliability Corporation "may take effect no earlier than 31 days after [the Reliability Corporation] files with [FERC] [the] notice of penalty and record of the proceedings." 16 U.S.C. § 824o(e)(2); *see also* 18 C.F.R. § 38.7(e). The Federal Power Act further states that "[s]uch penalty shall be subject to review by [FERC], on its own motion or upon application by the user, owner or operator that is the subject of the penalty filed within 30 days after the date such notice is filed with [FERC]." *Id.*

Historically, the Reliability Corporation has filed a batch of Notices of Penalty at the end of each calendar month, a typical batch ranging from 75 to 120 Notices. Kuehnle Decl. ¶ 10. The Reliability Corporation's typical practice has been to file the Notices of Penalty pertaining to violations of the Reliability Standards that involve grid operations (e.g., vegetation management and balancing generation and load) as a public document without seeking a Critical Energy Infrastructure Information designation. *Id.* For violations of the Reliability Standards that pertain to cyber security or physical security of the electric grid, the Reliability Corporation historically requested that certain information be designated as Critical Energy Infrastructure Information. *Id.* The Reliability Corporation's public version of a Critical Infrastructure Protection-related Notice of Penalty does not contain the names of the relevant Entities and contains less detail regarding

violations to avoid the disclosure of information that would be useful to individuals targeting attacks directed at critical electric infrastructure. *Id.* In contrast, the non-public Notices of Penalties contain the names of Entities found to have violated the Reliability Standards as well as additional details regarding the nature of the relevant violations. *Id.*

C. Plaintiff's FOIA Requests.

The three FOIA requests from Plaintiff at issue were designated by the Agency as FOIA Nos. FY19-19; FY19-30; and FY19-99 (collectively, the "Requests"), and seek the disclosure of the identities of approximately 1,500 Entities and their actual or potential non-compliance with the Reliability Corporation's cybersecurity Reliability Standards. Initially, Plaintiff's Requests sought the non-public version Notice of Penalties, which include the names of relevant Entities and contain additional details regarding the violations excluded from the public version. However, "FERC staff proposed and Plaintiff agreed to reduce the scope of the FOIAs to the cover page of each publicly available Notice of Penalty with the names(s) of the violator(s) and the docket number inserted on the first page." Compl. ¶ 25. In essence, Plaintiff withdrew his request for the non-public Notices of Penalty and now seeks only the public versions, along with the names of previously withheld Entities inserted therein.

Following receipt of the Requests, FERC staff assessed each Critical Infrastructure Protection Notice of Penalty on a rolling basis to determine whether the disclosure of the relevant Entities as to each was appropriate under the FOIA. Following receipt of certain determinations denying the release of Entity identities, Plaintiff filed an appeal with the Agency. The appeal was denied, and Plaintiff filed the instant lawsuit on November 15, 2019. Pursuant to the Court's orders—*see* Jan. 28, 2020, Minute Order; ECF No. 35—FERC continued its rolling processing of the relevant Notices of Penalty and concluded such processing on January 31, 2022. *See* ECF

No. 38. Ultimately, FERC disclosed Entity identities associated with the 253 Notices of Penalty. FERC also withheld some entity identities, relying on Exemptions 3 and 7(F).

Although certain Entity identities were released—in instances in which FERC determined that disclosure would not pose an undue risk to the bulk electric system—Plaintiff maintains that all Entity identities associated with the 253 separate FERC docket numbers should be made available via FOIA. In this regard, Plaintiff does not dispute FERC's rationale for the Exemptions; instead, Plaintiff's position is that the disclosure of Entity identities and associated penalties will serve as an incentive for their compliance with the Reliability Standards. *See* Compl, ECF No. 1, ¶ 21 ("At the heart of the public understanding whether or not the enforcement of these [Critical Infrastructure Protection] standards is adequate, lies the need for the names of regulatory violators to be released. Without this information, neither the public, investors, Congress nor state regulators can hold utilities accountable for protecting the portion of the electric grid that these utilities own or operate. In fact, Plaintiff believes there is little incentive for companies to do more than the minimum—if even that—to protect the grid absent public scrutiny."); Mabee Decl., ECF No. 34-1, ¶ 22 ("Ending the coverup of the identities of regulatory violators—which is obscuring the failures of the regulatory regime from the public, Congress and state regulators—is much more urgent[.]"). In essence, Plaintiff believes that withholding the identities of the relevant Entities does more harm than would publishing their identities for all to see—along, of course, with the already publicly available Notices of Penalty and associated additional detail regarding the violations.

The parties are in accord on the danger faced by the nation's electric infrastructure from the threat of cyberattack. As set forth in a recent Government Accountability Office Report, the energy grid's distribution systems "face significant cybersecurity risks—that is, threats,

vulnerabilities, and impacts—and are increasingly vulnerable to cyberattacks." GAO-21-81 Electricity Grid Cybersecurity (March 2021). As further noted by the Government Accountability Office, "[t]hreat actors are growing more adept at exploiting these vulnerabilities to execute cyberattacks." *Id.* Indeed, Plaintiff himself has recognized the real threat posed by cyber security intrusion, asserting that "state actors such as Russia and China have penetrated the U.S. electric grid for over a decade." FERC Docket AD19-18 (comments of Michael Mabee on the role of transparency in preventing regulatory failures under AD19-18, Accession No. 20191028-5003). The parties differ, however, in their views regarding the danger that disclosure of the Entities would pose to the electric grid. FERC's staff, composed of electrical engineers, computer engineers, cyber security personnel, Reliability Standard experts, and other technical experts, caution that release of the withheld Entities would reveal information that could be used by nefarious individuals to harm the electric grid. Plaintiff disagrees asserting, without evidence submitted at the administrative appeal, that disclosure may help encourage compliance. *See generally* Compl.

LEGAL STANDARDS

Summary judgment is appropriate when the pleadings and evidence "show[ ] that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). The party seeking summary judgment must demonstrate the absence of a genuine issue of material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). A genuine issue of material fact is one that "might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). Once the moving party has satisfied its burden, the nonmoving party "may not rest upon the mere allegations or denials of his pleadings, but . . . must set forth specific facts showing that there is a genuine issue for trial." *Id.* at 248.

The "vast majority" of FOIA cases are decided on motions for summary judgment. *Brayton v. Off. of U.S. Trade Rep*., 641 F.3d 521, 527 (D.C. Cir. 2011); *see also Media Rsch. Ctr. v. Dep't of Just.*, 818 F. Supp. 2d 131, 136 (D.D.C. 2011) ("FOIA cases typically and appropriately are decided on motions for summary judgment"); *Citizens for Resp. & Ethics in Wash. ("CREW") v. Dep't of Lab.*, 478 F. Supp. 2d 77, 80 (D.D.C. 2007). An agency may be entitled to summary judgment in a FOIA case if it demonstrates that no material facts are in dispute, it has conducted an adequate search for responsive records, and each responsive record that it has located either has been produced to the plaintiff or is exempt from disclosure. *See Weisberg v. Dep't of Just.*, 627 F.2d 365, 368 (D.C. Cir. 1980).

To meet its burden, a defendant may rely on reasonably detailed and non-conclusory declarations. *See McGehee v. CIA*, 697 F.2d 1095, 1102 (D.C. Cir. 1983); *Media Rsch. Ctr.*, 818 F. Supp. 2d at 137. "[T]he Court may award summary judgment solely on the basis of information provided by the department or agency in declarations when the declarations describe 'the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith.'" *CREW*, 478 F. Supp. 2d at 80 (quoting *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981)). "[A]n agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Media Rsch. Ctr.*, 818 F. Supp. 2d at 137 (quoting *Larson v. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir. 2009)).

ARGUMENT

In FERC's good faith assessment, the disclosure of the withheld Entity identities sought by Plaintiff would reveal cybersecurity-related information that would be useful to bad actors

seeking to target the nation's critical infrastructure. Further, the identities are categorically exempt under FOIA Exemption 3, because they constitute Critical Energy/Electric Infrastructure Information and are exempt from disclosure under the FAST Act. Additionally and alternatively, the same information is exempt from disclosure under Exemption 7(F) because the identities also constitute "law enforcement information," the disclosure of which could reasonably be expected to endanger the life or physical safety of any individual—here, those connected to the impacted portion of the power grid impaired by an attack. FERC has explained the foreseeable harm that would flow from disclosure of the withheld Entities' identities.

A. Critical Energy/Electric Infrastructure Information is Exempt from Disclosure Under the FAST Act

Exemption 3 allows agencies to withhold information that is already prohibited from disclosure by another statute. 5 U.S.C. § 552(b)(3). "Exemption 3 differs from other FOIA exemptions in that its applicability depends less on the detailed factual contents of specific documents; the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within that statute's coverage." *Goland v. CIA*, 607 F.2d 339, 350 (D.C. Cir. 1978).

On December 4, 2015, the FAST Act was signed into law. Among other provisions, the FAST Act added section 215A to the Federal Power Act to improve the security and resilience of energy infrastructure in the face of emergencies. In doing so, Congress included the following definition of "Critical Electric Infrastructure Information" within the statute:

> The term "critical electric infrastructure information" means information related to critical electric infrastructure,[5] or proposed critical electrical infrastructure,

[5] Under the FAST Act, Congress defined "Critical Electric Infrastructure" 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." 16 U.S.C. § 824o-1 (emphasis added).

> generated by or provided to the [Federal Energy Regulatory] Commission or other Federal agency, 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 Commission's regulations.

16 U.S.C. § 824o–1(a)(3). The FAST Act also directed the Commission to issue regulations that provide: (1) the criteria and procedures for designating information as Critical Electric Infrastructure Information; (2) a specific prohibition on unauthorized disclosure of Critical Electric Infrastructure Information; (3) sanctions for the knowing and willful unauthorized disclosure of Critical Electric Infrastructure Information by Commission and Department of Energy employees; and (4) a process for voluntary sharing of Critical Electric Infrastructure Information. 16 U.S.C. § 824o-1(d)(2).

Under the FAST Act, Critical Electric Infrastructure Information, which includes information under FERC's regulatory definition of Critical Energy Infrastructure Information, is exempt from disclosure pursuant to FOIA Exemption 3: Critical Electric Infrastructure Information "shall be exempt from disclosure under Section 552(b)(3) of Title 5." 16 U.S.C. § 824o-1(d)(1)(A); *see also Union of Concerned Scientists v. Dep't of Energy*, 998 F.3d 926, 927 (D.C. Cir. 2021) (noting that Critical Electric Infrastructure Information is exempt from disclosure under FOIA). Indeed, Congress has made it a sanctionable offense for FERC, its employees, or its agents to disclose Critical Electric Infrastructure Information. 16 U.S.C. § 824o-1(d)(2)(C). Pursuant to Congress' direction, on November 17, 2016, FERC issued Order No. 833, which amended the Agency's regulations at 18 C.F.R. §§ 375.309, 375.313, 388.112, and 388.113 to implement the FAST Act provisions that pertain to the designation, protection and sharing of Critical Electric Infrastructure Information. Order No. 833 also revised the Agency's existing Critical Energy Infrastructure Information regulations. In amending its regulations, FERC

adopted Congress' own definition of "Critical Electric Infrastructure Information" set forth above. Notably, both the FAST Act as well as the Commission's amended regulations define "critical infrastructure" identically 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." 16 U.S.C. § 824o–1(a)(2); 18 C.F.R. § 388.113(c)(3).

In addition to promulgating a definition of Critical Electric Infrastructure, as directed by the FAST Act the Agency's regulations also set forth a definition of "Critical Energy Infrastructure Information," as specific 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.

See 18 C.F.R. § 388.113. Once information has been designated as Critical Electric Infrastructure Information pursuant to FERC's regulations, that information must not be disclosed. *See* 16 U.S.C. §§ 824o-1(d)(1), (d)(2)(C), (d)(6).

B. <u>The Withheld Entity Identities are Protected from Disclosure by Exemption 3.</u>

The FAST Act and its implementing regulations require the withholding of the requested Entity names. Critical to the Court's analysis is the fact that the public Notices of Penalty relating to the withheld Entity identities may be accessed by anyone via FERC's public docket. *See* Kuehnle Decl. ¶ 10. As a result, the disclosure of the Entity identities, when combined with public information about the vulnerabilities of the Entities set forth in the publicly available Notices of

Penalty, would be useful to those seeking to target the nation's electric grid. *See Sussman v. Marshals Serv.*, 494 F.3d 1106, 1116 (D.C. Cir. 2007) (acknowledging that a FOIA release "would release the contested materials to *the world at large*, not just to [the requestor]") (emphasis in original); *see also Reps. Comm. for Freedom of Press v. FBI*, Civ. A. No. 17-1701 (RC), 2022 WL 13840088, at *7 (D.D.C. Oct. 21, 2022) (accepting as "logical and plausible" agency's "mosaic theory, which posits that seemingly innocuous information 'when taken together' in the aggregate could reveal protected information, a potential lawbreaker could piece together this information to draw conclusions" that could endanger the public). Indeed, Plaintiff is not merely seeking "names" of Entities, but rather he is seeking names of Entities that can be examined in concert with certain details surrounding the violations set forth in each publicly available Notice of Penalty. *Id.* ¶¶ 12, 17-18. For this reason, FERC's analysis of whether disclosure of each Entity name was appropriate involved an examination of information that is already publicly available within the public Notice of Penalty. *Id.* ¶ 14. Additional factors considered by FERC included the following:

- The nature of the Reliability Standard violation, including whether there is a Technical Feasibility Exception[6] involved that does not allow the Entity to fully meet the standards;
- whether vendor-related information is contained in the Notices of Penalty;
- whether mitigation is complete;

[6] There are certain cybersecurity compliance standards for which compliance is not possible from a technical perspective. In such instances, entities may seek a Technical Feasibility Exception. Some of the public Notices of Penalty reveal the existence of these exceptions in an Entity's cyber security environment. Thus, even when the other violations set forth in such a Notice of Penalty have been mitigated, the disclosure of the relevant Entity identity in concert with the public Notice of Penalty will inform bad actors of a Technical Feasibility Exception vulnerability associated with that particular Entity's network. For example, exceptions are sought by Entities for certain "legacy devices" that do not have the capacity to meet current security standards. For instance, some devices can only accept four-character passwords and cannot be enhanced. Unfortunately, four-character passwords are relatively easy to crack.

- the extent to which the disclosure of the identity of the Entity and other information would be useful to someone seeking to cause harm;
- whether a successful audit has occurred since the violation(s);
- whether the violation(s) was (were) administrative or technical in nature; and
- the length of time that has elapsed since the filing of the public Notice of Penalty.

FERC's FOIA office, working with expert staff, applied the above criteria to scrutinize each noncompliance and determine the risks of public disclosure. *Id.* ¶¶ 13, 15. In instances in which staff determined that disclosure of an identity would be useful to planning an attack on critical infrastructure based on its analysis, the Agency withheld such names, relying upon Exemptions 3 and7(F). *Id*. ¶ 15. In instances in which FERC staff concluded that disclosure of an Entity's name would not be useful for such an attack, the name was disclosed in conjunction with the public Notice of Penalty. Thus, in response to Plaintiff's request, where FERC determined that there was no material risk, names were disclosed to Plaintiff, but were withheld if FERC determined that they would be useful to someone "seeking to cause harm to the electric grid," among other factors. Kuehnle Decl. ¶¶ 13-15.

In sum, FERC determined that disclosing the names of these Entities in violation of cyber security standards would create a risk of harm or a detriment to life, physical safety, or security. *See, e.g.*, Feb. 22, 2021, letter. The violations by the Entities directly bear upon control room functions tied to electrical transmission, and thus linking specific knowledge of these cybersecurity violations to specific Entities would increase the risk to critical energy infrastructure under their control. Kuehnle Decl. ¶ 17. In this regard, it is worth noting that, as asserted in Plaintiff's Complaint, he regularly posts materials received from FERC on his "blog," which is available to both concerned citizens and bad actors alike.

Accordingly, FERC properly concluded that the Entity identities at issue constitute Critical Energy Infrastructure Information and are exempt from disclosure under Exemption 3. Disclosing the names sought by Plaintiff would reveal specific vulnerabilities potentially useful to a person in planning an attack on critical infrastructure, and thus the Critical Energy Infrastructure Information-designated information falls squarely within the scope of the material required to be withheld by the FAST Act. Finally, FERC is entitled to deference in connection with its determination as to the application of Exemption 3. *See Morley v. CIA*, 699 F. Supp. 2d 244, 254 (D.D.C. 2010), *aff'd in part, vacated in part*, 466 F. App'x 1 (D.C. Cir. 2012) (noting that "agencies are owed special deference when they invoke Exemption 3," and stating that the D.C. Circuit has held that "Exemption 3 differs from other FOIA exemptions in that its applicability depends less on the detailed factual contents of specific documents; the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within the statute's coverage.") (quoting *Ass'n of Retired R.R. Workers v. U.S. R.R. Ret. Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987)); *Broward Bulldog, Inc. v. Dep't of Just.*, 939 F.3d 1164 (11th Cir. 2019) (holding that district court owes substantial deference to federal agency's invocation of FOIA Exemption 3 for information specifically exempted from disclosure by statute if statute affords agency no discretion on disclosure, even though agency still bears burden of proving applicability of that exemption). As in those other instances, Congress has afforded FERC no discretion with respect to disclosure of Critical Electric Infrastructure Information, enacting into the FAST Act itself specific language exempting such information from the disclosure requirements of FOIA and making it a sanctionable offense to improperly disclose such information. *See* 16 U.S.C. §§ 824o-1(d)(1)(A), (d)(2)(C), (d)(6); *Union of Concerned Scientists*, 998 F.3d at 927.

C. The Withheld Entity Identities are Protected from Disclosure by Exemption 7(F).

Exemption 7(F) protects from disclosure "records or information compiled for law enforcement purposes [the disclosure of which] could reasonably be expected to endanger the life or physical safety of any individual" 5 U.S.C. § 552(b)(7)(F).

1. The Entity Identities Constitute "Law Enforcement Information."

Courts have routinely interpreted the term "law enforcement" broadly for purposes of FOIA Exemption 7 to include civil, as well as criminal law enforcement objectives. Thus, for example, in *Public Employees for Environmental Responsibility ("PEER") v. U.S. Section, International Boundary & Water Commission U.S-Mexico*, 740 F.3d 195, 203 (D.C. Cir. 2014), the D.C. Circuit held that the term "law enforcement" includes proactive steps to prevent criminal activity and maintain security and the prevention of terrorism. *Id.* Similarly, in *Sack v. Department of Defense*, 823 F. 3d 687, 694 (D.C. Cir. 2016), the D.C. Circuit held that "Exemption 7 uses the term 'law enforcement' to describe 'the act of enforcing the law, both civil and criminal.'" *Id.* This Court has emphasized that "FERC certainly meets that description" as a law enforcement agency. *STS Energy Partners LP v. FERC*, 82 F. Supp. 3d 323, 333 (D.D.C. 2015) (upholding reliance by FERC on Exemption 7 to withhold certain records relating to an ongoing investigation).

In the instant case, pursuant to Congress' direction, FERC certified the Reliability Corporation as the designated Electric Reliability Organization with the responsibility of developing, auditing, and enforcing the cybersecurity Reliability Standards at issue.[7] *See* Kuehnle

[7] The statutory definition of reliability standard is set forth at Federal Power Act section 215(a)(3), 16 U.S.C. § 824o(a)(3):

> The term "reliability standard" means a requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable

Decl. ¶ 8. FERC has corresponding oversight of such enforcement efforts via its ability to review Notices of Penalty. In short, the Entity identities at issue clearly constitute "law enforcement information."

2. The Disclosure of the Withheld Entity Identities Could Reasonably be Expected to Endanger the Life or Physical Safety of Individuals.

As discussed, the Entity identities sought by Plaintiff relate directly to the Reliability Corporation's cybersecurity Reliability Standards that are designed to ensure the protection of the national electric infrastructure from both state and non-state actors. *See* Kuehnle Decl. ¶ 17. The harm associated with an attack on a particular critical infrastructure asset would include, among others, those undergoing treatment at hospitals; first responders and those whom they serve; and even those simply relying upon traffic control in their daily commute. *Id*. In this regard, the term "any individual" has been interpreted to encompass third parties reasonably at risk of harm, even when it was not possible to identify the specific individuals whose safety is at risk. *See Elec. Privacy Info. Ctr. v. Dep't of Homeland Sec.*, 777 F.3d 518, 525 (D.C. Cir. 2015). Additionally, the D.C. Circuit has held that disclosure "need not definitely endanger life or physical safety; a reasonable expectation of endangerment suffices." *PEER*, 740 F.3d at 206; *accord Friedman v. Secret Serv.*, 282 F. Supp. 3d 291, 307 (D.D.C. 2017) (quoting *PEER*, 740 F.3d at 205).

Here, the assessment of facts demonstrating danger mirrors that in *Living Rivers, Inc. v. Bureau of Reclamation*, 272 F. Supp. 2d 1313, 1321-22 (D. Utah 2003), where a district court found that disclosing "inundation maps" produced to model flooding after dam breaches

---

> operation of the bulk-power system, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.

Id.

reasonably posed a risk of danger to the lives of individuals living in downstream areas. The court reasoned that such information "could increase the risk of attack" by enabling bad actors to identify targets for maximal damage. *Id.* at 1321-22. Similarly here, publicly disclosing the names of Entities in violation of the Reliability Corporation's Reliability Standards pertaining to cybersecurity increases the risk of cyberattack by linking vulnerabilities to specific electric utility companies. Again, such violations include, by way of example, the failure to properly list critical cyber assets, the failure to timely provide applicable cybersecurity training following grant of access to critical cyber assets, failure to implement appropriate "patching" or testing of hardware and software, and the failure to conduct risk assessments of contract employees, including some with access to critical cyber assets. Such information, gathered over time, could render Entities vulnerable on the basis of future cybersecurity shortfalls connected with these same transmission control rooms. Along these lines, Plaintiff apparently contends that the completion of mitigation of a particular violation necessarily means that disclosure of the Entity's identity is appropriate. In FERC's experience and judgment, this is not the case. Simply because specified mitigation has been completed does not mean that the vulnerability has been fully addressed; it may take time to properly assess whether an entity's efforts to address the relevant threat or issue have been successful. Kuehnle Decl. ¶¶ 14, 17-18.

Finally, an agency's assessment of danger when applying Exemption 7(F) is typically accorded deference within limits. *See Garcia v. Dep't of Just.*, 181 F. Supp. 2d 356, 378 (S.D.N.Y. 2002) ("In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger."). In determining whether the disclosure of an Entity's identity associated with a particular Notice of Penalty docket is appropriate, FERC engaged in a case-by-case assessment, examining a variety of factors, including those set forth

above in Section IV.A. While Plaintiff may believe that FERC's determinations will cause more harm than good, such disagreement does not form the basis for second-guessing the expert agency's decisions. *See Greenpeace, Inc. v. Dep't of Homeland Sec.*, 311 F. Supp. 3d 110, 130 (D.D.C. 2018) ("Therefore, DHS is not required to show that risks to human life and health from potential terrorist attacks outweigh the possibility that withholding the information might inhibit the development of best practices by the private sector.").

CONCLUSION

For the foregoing reasons, the Court should grant FERC summary judgment.

Dated: March 5, 2024
Washington, DC

Respectfully submitted,

MATTHEW M. GRAVES
D.C. Bar No. #481052
United States Attorney

BRIAN P. HUDAK
Chief, Civil Division

By: */s/ Kartik N. Venguswamy*
KARTIK N. VENGUSWAMY
D.C. Bar No. #983326
Assistant United States Attorney
601 D Street, NW
Washington, D.C. 20530
Tel: (202) 252-1790
kartik.venguswamy@usdoj.gov

Attorneys for the United States of America

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL MABEE, Plaintiff, v. FEDERAL ENERGY REGULATORY COMMISSION, Defendant.	Civil Action No. 19-3448 (ACR)

[PROPOSED] ORDER

UPON CONSIDERATION of the Defendant's Motion for Summary Judgement, and the entire record in this matter, it is hereby:

ORDERED that the Defendant's Motion is GRANTED; and it is further

ORDERED that summary judgment is entered in favor of Defendant.

Dated: _____

_____
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL MABEE,

Plaintiff,

v.

FEDERAL ENERGY REGULATORY COMMISSION,

Defendant.

Civil Action No. 19-3448 (ACR)

DEFENDANT'S STATEMENT OF MATERIAL FACTS
AS TO WHICH THERE IS NO GENUINE DISPUTE

Defendant, Federal Energy Regulatory Commission ("FERC"), by and through undersigned counsel, respectfully submits in support of its motion for summary judgment this statement of material facts as to which there is no genuine dispute.

Security of the Nation's Electric Grid.

1. On July 20, 2006, NERC was certified by FERC pursuant to authority delegated under section 215 of the Federal Power Act as the nation's designated Electric Reliability Organization. 116 FERC ¶ 61,062. Upon this certification, NERC became responsible for, among other things, the development and enforcement of reliability standards designed to, as the name implies, maintain the reliability of the United States' electric grid. *Id.* Such reliability standards include requirements associated with ensuring the physical security of electric infrastructure as well as requirements associated with ensuring the integrity of electric cyber security infrastructure. *Id.*; Kuehnle Decl. ¶ 8. By way of example, the reliability standards at issue here—the Critical Infrastructure Protection Reliability Standards—address matters such as background checks for

employees with access to critical cyber assets and assuring that electric utilities and other industry stakeholders timely install security patches to protect software and adequately train electric utility staff on cyber security response measures. Kuehnle Decl. ¶ 8.

2. NERC, together with its six "Regional Entities" located throughout the United States and Canada, conducts audits and other assessments[1] regarding electric utility companies' compliance with the Reliability Standards. *Id.* ¶ 9. Part of the enforcement actions for the non-compliance are mitigation plans and, where appropriate, monetary penalties. *Id.*

B. NERC Notices of Penalty.

3. Upon completion of an audit, NERC and the Regional Entities may refer audit findings to their enforcement staff as potential violations of the Reliability Standards. *Id.* ¶ 10.

4. Upon a finding of a violation and determination of a monetary penalty—or, more often settlement with the alleged violator—NERC then files a "Notice of Penalty" with FERC. *Id.*; *see also* 16 U.S.C. § 824o(e)(2); 18 C.F.R. § 38.7(e). Section 215(e)(2) of the Federal Power Act provides that a penalty submitted by NERC "may take effect no earlier than 31 days after NERC files with [FERC] [the] notice of penalty and record of the proceedings." 16 U.S.C. § 824o(e)(2); *see also* 18 C.F.R. § 38.7(e). The Federal Power Act further states that "[s]uch penalty shall be subject to review by [FERC], on

[1] Other assessments include, by way of example, self-certifications, spot-checks, compliance investigations, self-reporting, and self-logging. These assessment tools, as well as other aspects of other aspects of NERC's Compliance Monitoring and Enforcement Program, are set forth in Appendix 4C of the NERC Rules of Procedures found at https://www.nerc.com/AboutNERC/RulesOfProcedure/NERC_ROP_With_Appendices.pdf

its own motion or upon application by the user, owner or operator that is the subject of the penalty filed within 30 days after the date such notice is filed with [FERC]." *Id.*

5. Historically, NERC has filed a batch of Notices of Penalty at the end of each calendar month, a typical batch ranging from 75 to 120 Notices. Kuehnle Decl. ¶ 10. NERC's typical practice has been to file the Notices of Penalty pertaining to violations of the Reliability Standards that involve grid operations (*e.g.*, vegetation management and balancing generation and load) as a public document without seeking a Critical Energy Infrastructure Information designation. *Id.* For violations of the Reliability Standards that pertain to cyber security or physical security of the electric grid, NERC historically requested that certain information be designated as Critical Energy Infrastructure Information. *Id.* NERC's public version of a Critical Infrastructure Protection-related Notice of Penalty does not contain the names of the relevant Entities and contains less detail regarding violations in order to avoid the disclosure of information that would be useful to individuals targeting attacks directed at critical electric infrastructure. *Id.* In contrast, the non-public Notices of Penalties contain the names of Entities found to have violated the Reliability Standards as well as additional details regarding the nature of the relevant violations. *Id.*

C. <u>Plaintiff's FOIA Requests.</u>

6. The three FOIA requests from Plaintiff at issue were designated by the Agency as FOIA Nos. FY19-19; FY19-30; and FY19-99 (collectively, the "Requests"), and seek the disclosure of the identities of approximately 1,500 Entities and their actual or potential non-compliance with NERC cyber-security Reliability Standards. Initially, Plaintiff's Requests sought the non-public versions of Notices of Penalties, which include the

names of relevant Entities and contain additional details regarding the violations excluded from the public versions. However, "FERC staff proposed and Plaintiff agreed to reduce the scope of the FOIAs to the cover page of each publicly available Notice of Penalty with the names(s) of the violator(s) and the docket number inserted on the first page." Compl., ECF No. 1, ¶ 25. In essence, Plaintiff withdrew his request for the non-public Notices of Penalty and now seeks only the public versions, along with the names of previously-withheld Entities inserted therein.

7. Following receipt of the Requests, FERC staff assessed each Critical Infrastructure Protection Notice of Penalty on a rolling basis to determine whether the disclosure of the relevant Entities as to each was appropriate under the FOIA. Following receipt of certain determinations denying the release of Entity identities, Plaintiff filed an appeal with the Agency. The appeal was denied, and Plaintiff filed the instant lawsuit on November 15, 2019. Pursuant to the Court's orders—*see* Jan. 28, 2020, Minute Order; ECF No. 35—FERC continued its rolling processing of the relevant Notices of Penalty and concluded such processing on January 31, 2022. *See* ECF No. 38. Ultimately, FERC disclosed Entity identities associated with the 253 Notices of Penalty. Relying on Exemptions 3 and 7(F), FERC also withheld some entity identities. 5 U.S.C. §§ 552(b)(3), (b)(7)(F).

8. Although certain Entity identities were released—in instances in which FERC determined that disclosure would not pose an undue risk to the bulk electric system—Plaintiff maintains that all Entity identities associated with the 253 separate FERC docket numbers should be made available via FOIA. In this regard, Plaintiff does not dispute FERC's rationale for the Exemptions; instead, Plaintiff's position is that the

disclosure of Entity identities and associated penalties will serve as an incentive for their compliance with the Reliability Standards. *See* Compl, ECF No. 1, ¶ 21 ("At the heart of the public understanding whether or not the enforcement of these CIP standards is adequate, lies the need for the names of regulatory violators to be released. Without this information, neither the public, investors, Congress nor state regulators can hold utilities accountable for protecting the portion of the electric grid that these utilities own or operate. In fact, Plaintiff believes there is little incentive for companies to do more than the minimum – if even that – to protect the grid absent public scrutiny."); Mabee Decl., ECF No. 34-1, ¶ 22 ("Ending the coverup of the identities of regulatory violators – which is obscuring the failures of the regulatory regime from the public, Congress and state regulators – is much more urgent[.]"). In essence, Plaintiff believes that withholding the identities of the relevant Entities does more harm than would publishing their identities for all to see—along, of course, with the already publicly available Notices of Penalty and associated additional detail regarding the violations.

9. The parties are in accord on the danger faced by the nation's electric infrastructure from the threat of cyber-attack. As set forth in a recent Government Accountability Office ("GAO") Report, the energy grid's distribution systems "face significant cybersecurity risks—that is, threats, vulnerabilities, and impacts—and are increasingly vulnerable to cyberattacks." GAO-21-81 Electricity Grid Cybersecurity (March 2021). As further noted by GAO, "[t]hreat actors are growing more adept at exploiting these vulnerabilities to execute cyberattacks." *Id.* Plaintiff himself has recognized the real threat posed by cyber security intrusion, asserting that "state actors such as Russia and China have penetrated the U.S. electric grid for over a decade." *See* FERC Docket

AD19-18 (comments of Michael Mabee on the role of transparency in preventing regulatory failures under AD19-18, Accession No. 20191028-5003).

10. The parties differ, however, in their views regarding the danger that disclosure of the Entities would pose to the electric grid. FERC's staff, composed of electrical engineers, computer engineers, cyber security personnel, Reliability Standard experts, and other technical experts, caution that release of the withheld Entities would reveal information that could be used by nefarious individuals to harm the electric grid. Kuehnle Decl. ¶¶ 17-18.

11. Plaintiff disagrees, asserting, without evidence submitted at the administrative appeal, that disclosure may encourage compliance. *See generally* Compl., ECF Doc. No. 1.

Dated: March 4, 2024
Washington, DC

Respectfully submitted,

MATTHEW M. GRAVES
D.C. Bar No. #481052
United States Attorney

BRIAN P. HUDAK
Chief, Civil Division

By: */s/ Kartik N. Venguswamy*
KARTIK N. VENGUSWAMY
D.C. Bar No. #983326
Assistant United States Attorney
601 D Street, NW
Washington, D.C. 20530
Tel: (202) 252-1790
kartik.venguswamy@usdoj.gov

Attorneys for the United States of America

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Michael Mabee Plaintiffs, v. FEDERAL ENERGY REGULATORY COMMISSION, Defendant.	)	Civil Action No. 1:19-cv-03448

DECLARATION OF BARRY W. KUEHNLE

1. I, BARRY W. KUEHNLE, Energy Infrastructure and Cyber Security Advisor, within the Office of Electric Reliability at the Federal Energy Regulatory Commission ("FERC" or "Agency"), declare that the following statements are true and correct to the best of my knowledge and belief and that they are based upon my personal knowledge and experience and on information supplied to me by employees under my lead and employees in other FERC offices.

Background and Experience

2. In May of 1996, I enlisted in the United States Navy with a special duty assignment in the field of Military Intelligence. As assigned by the U.S. Navy, I continued to work toward a Bachelor of Science Degree in Computer Engineering. In January 1998, I graduated from Case Western Reserve University with a degree in Computer Engineering. In January 1999, I was assigned to the Naval Information Warfare Activity where I served as a Project Manager—Computer Engineer and Intelligence Officer.

3. After leaving the Navy, I worked as a Project Coordinator—Computer Engineer for the United States Department of Defense ("DoD"), Defense Technology Analysis Office from April 2002 until May 2005. I then worked as a Critical Infrastructure Security Engineer and Computer Engineer in the private sector from May 2005 until February 2006. I then worked for Battelle Energy Alliance for Idaho National Laboratory in the role of Critical Infrastructure Protection Center Director from February 2006 until January 2008. In January 2008, I served as a Critical Infrastructure Protection Analyst for DoD's Defense Technology Analysis Office again. In this role, I was the Idaho Division Chief for Critical Infrastructure Protection.

4. In August 2010, I joined FERC in the Office of Electric Reliability ("OER") and in December 2012 transferred to the Office of Energy Infrastructure Security ("OEIS") as an Energy Infrastructure and Cyber Security Advisor. OIES' responsibilities include providing leadership, expertise and assistance to the Commission to identify, communicate, and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyber attacks that would impact the reliability of the bulk power system.

5. In February 2016, I transferred from OEIS back to FERC's Office of Electric Reliability ("OER") as an Executive Service Energy Infrastructure and Cyber Security Advisor. OER assists in the protection and improvement of the reliability and security of the nation's bulk power system through effective regulatory oversight as established by Congress and the President in the Energy Policy Act of 2005. OER also oversees the development and review of mandatory reliability and security standards, as well as compliance with the approved mandatory standards by the users, owners, and operators of the bulk power system. In my current role with OER, my responsibilities include, among others, providing analysis, technical input, and development and review of Orders, filings, Notices of Penalty, Notices of Inquiry, and internal Commission

memoranda for the development and modification of Critical Infrastructure Protection ("CIP") Reliability Standards. I also prepare technical cyber security public reports, notifications, and related documents which analyze threats and vulnerabilities. Additionally, I participate in cyber security audits as a technical lead to verify compliance with North American Reliability Corporation ("NERC") CIP Reliability Standards. I currently hold a TS/SCI clearance with a counterintelligence polygraph. I also regularly receive classified briefings and keep abreast of developments relating to cyber threats, including those targeting critical infrastructure.

6. I am experienced in a number of computer programming languages, networking design and configuration, access management and controls, cyber system monitoring, as well as cyber security design, implementation, incident response and recovery.

NERC Notices of Penalty and Enforcement of Reliability Standards

7. As noted above, I have been employed with FERC since 2010 in the roles previously discussed and as a result, have familiarity with the NERC Notice of Penalty[1] audit, preparation, and filing processes.

8. NERC is the FERC-designated Electric Reliability Organization, which is responsible for the development and enforcement (subject to Commission review) of Reliability Standards relating to physical security and cyber security related CIP standards. Examples of CIP Reliability standards include conducting background checks for employees who have access to critical cyber assets, *see* CIP-004-6 R3, ensuring that electric utilities timely install cyber security patches to protect software, *see* CIP-007-6 R2, and ensuring proper protections are in place to

[1] There are three variations of a penalty filing: the "Find, Fix, and Track Report," the "Notice of Penalty," and the "Spreadsheet Notice of Penalty." A "Find, Fix, and Track Report" and "Spreadsheet Notice of Penalty" generally address numerous Unidentified Registered Entities or "UREs" and associated violations within a single document. "A Notice of Penalty" generally addresses one URE and certain related violations. For purposes of this declaration, I will refer to all of the foregoing variations of penalty filings collectively by the term "Notice of Penalty."

permit only necessary communications to the cyber systems protected by the CIP Reliability standards, *see* CIP-005-6 R1.

9. NERC, along with its six "Regional Entities," located throughout the United States and Canada, conducts audits and other assessments regarding electric utility companies' compliance with Reliability Standards. Enforcement actions for non-compliance include mitigation plans and in certain cases, monetary penalties.

10. Upon completion of a Reliability Standard audit, NERC and the Regional Entities may refer audit findings to their corresponding enforcement staff. Upon determination of a monetary penalty, remedial action, or settlement, NERC then files a Notice of Penalty with FERC. Historically, NERC has filed batches of Notices of Penalty at the end of the calendar year, ranging from 75 to 120. In this regard, NERC's typical practice has been to file the Notices of Penalty pertaining to violations of Reliability Standards involving grid operations, such as vegetation management and balancing generation and load, as a public filing without seeking a Critical Energy/Electric or "CEII" designation. With respect to violations of CIP Reliability Standards that pertain to cyber security or physical security of the electric grid, NERC has requested that certain information be designated as CEII. NERC's public version of a CIP-related Notice of Penalty did not contain the names of the relevant entities and contained less detail regarding violations in order to avoid disclosure of information that would be useful to a state or non-state actor intending to carry out an attack on critical electric infrastructure. In contrast, non-public Notices of Penalties contain the names of entities found to have violated CIP-related Reliability Standards, as well as additional details regarding the nature of the violations.

Plaintiff's Freedom of Information Act Requests
(FOIA FY19-19, FY19-30, and FY19-99)

11. Upon FERC's receipt of Plaintiff's FOIA requests in December 2018, designated by the Agency as FOIA FY19-19, FY19-30, and FY19-99 ("Mabee FOIAs"), seeking information relating to non-public Notices of Penalty, I became involved with the technical review of the underlying Notices. I was also advised that Plaintiff modified his request to seek only the names of relevant previously Unidentified Registered Entities ("URE") in connection with the public Notices of Penalty, rather than the non-public Notices altogether.

12. Following FERC's initial receipt of the Mabee FOIAs, I personally performed the analysis of certain Notice of Penalty dockets in order to make a determination as to whether disclosure of relevant URE identities would create a material risk to the bulk electric system. Subsequently, Cathy Eade, a Critical Infrastructure Advisor in OER, began performing analyses of the UREs and associated dockets. Ms. Eade performed such analyses under my coordination and lead and she regularly met and consulted with me regarding her analyses and conclusions. As noted above, because NERC previously filed Notices of Penalty with the name of the entity omitted, but with certain information regarding the nature of the violation, a critical component of our analyses included examining the possible impact of the disclosure of a URE identity when paired with the already publicly available information contained within the public Notices of Penalty.

13. In order to ensure a consistent framework with respect to the analyses and conclusions, I, in collaboration with OER staff, including Ms. Eade and staff from FERC's General & Administrative Law section, developed a framework to reflect and document our analyses and conclusions. An example of a redacted copy of this documentation utilized for the Notices of Penalty and the associated UREs is attached is **Exhibit A** to this declaration.

14. In connection with FERC's analysis as to each Notice of Penalty docket and the associated UREs, the following factors were considered: the nature of the information contained in the publicly available version of the Notice of Penalty; the nature of the Critical Infrastructure Protection Reliability Standard violation, including whether there is a Technical Feasibility Exception involved that does not allow the URE to fully meet the CIP standards; whether vendor-related information is contained in the Notices of Penalty; whether mitigation is complete; the extent to which the disclosure of the identity of the URE and other information would be useful to someone seeking to cause harm; whether a successful 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.

15. Based on the application of the factors above and relying upon my experience, as well as the experience of Ms. Eade and OER staff, a conclusion and recommendation was made as to whether to disclose the identity of each URE. In certain cases, URE identities were disclosed. However, in the majority of instances, URE identities were withheld. My understanding is that FERC relied upon Exemption 3 (protected Critical Energy/Infrastructure Information) and Exemption 7(F) (protected law enforcement information the disclosure of which could reasonably harm an individual), in denying the release of the identities.

16. Given the volume of dockets and UREs involved, I am aware that the foregoing process was extremely time consuming. I am aware that in total, FERC spent in excess of 3,000 hours analyzing and processing these materials from December 2018 until the conclusion of its processing on January 31, 2022.

17. Based on my professional and technical experience, the withheld URE identities satisfy the definitional requirements of Critical Energy/Electric Information under the FAST Act,

as well as FERC's regulations. Further, I fully believe that the disclosure of the withheld URE identities could reasonably endanger the life or safety of others. In this regard, I am very familiar with the steps and measures that those seeking to cause harm to the electric grid will take to accomplish their efforts. For example, while the recent attack against the Colonial Pipeline did not specifically target the electric sector, the types of controls used to operate the electric grid are similar to those used at Colonial Pipeline. These systems are referred to as an Industrial Control System or "ICS." If an ICS is compromised, systems can be manipulated or even destroyed, leaving the ICS system inoperable and therefore affect the reliability of the grid. The impact of a critical infrastructure attack against the pipeline industry caused disruptions to public safety, among other things. If an attacker were to gain access to an electric grid system, it is reasonable to believe similar or worse impact would result. In this regard, unlike, for example, a storm-related outage, a cyber attack has no finite duration and may last, days, weeks, months, or longer. Additionally, a cyber attack is not limited to a geographical area and may simultaneously impact large portions of the United States. Extrapolating the outcome of Colonial Pipeline to dozens of utilities or more, the impact would affect the safety of potentially millions of Americans.

18. In those instances in which FERC withheld URE identities in connection with the Mabee FOIAs and associated Notices of Penalty, I believe and support the conclusion that the disclosure of such identities would create a material risk to the bulk electric system.

Pursuant to 28 U.S.C. § 1746, I hereby affirm under penalty of perjury that the foregoing declaration is true and correct.

Executed this _____

_____
Barry W. Kuehnle
Federal Energy Regulatory Commission

Exhibit A

1. Is a cybersecurity Technical Feasibility Exception(s) associated with this NOP?	☐ Yes ☐ No
2. Are there any outstanding enforcement actions or uncompleted mitigations plans associated with this NOP?	☐ Yes ☐ No
3. Has the Entity completed a subsequent audit? Please explain below:	☐ Yes ☐ No
4. Has the Entity completed other compliance activities (e.g., mitigation plans, enforcement actions, repeat alleged or confirmed violations) related to this NOP? Please explain below:	☐ Yes ☐ No
5. Would the technical assessment and risk analysis, in conjunction with releasing the Entity Name, reveal specific engineering, vulnerability, and/or detailed design information about the violator's system and therefore increase the risk to the BES?	☐ Yes ☐ No