

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL MABEE,

Plaintiff,

v.

Civil Action No. 19-3448 (FYP)

FEDERAL ENERGY REGULATORY
COMMISSION,

Defendant.

**DEFENDANT’S MEMORANDUM IN OPPOSITION TO PLAINTIFF’S CROSS-
MOTION FOR SUMMARY JUDGMENT AND REPLY IN SUPPORT OF
ITS MOTION FOR SUMMARY JUDGMENT**

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 opposition to Plaintiff’s cross-motion for summary judgment (ECF No. 43) and reply in support of the Agency’s motion for summary judgment.¹

PRELIMINARY STATEMENT

Plaintiff, Michael Mabee, made Freedom of Information Act, 5 U.S.C. § 552 (“FOIA”), requests to FERC for documents revealing the identities of various Unidentified Registered Entities who received notices of penalty for violations of the Critical Infrastructure Protection

¹ FERC inadvertently neglected to attach Exhibit A with the Kuehnle Declaration when submitting its Motion for Summary Judgment. After Plaintiff alerted FERC to this oversight, Defendant provided an unredacted copy of Exhibit A to Plaintiff on May 19, 2022. *See* Plaintiff’s Memorandum of Points and Authorities, ECF No. 42-9 (“Pl. Br.”) at 7 (noting that Defendant provided Plaintiff with Exhibit A on May 19, 2022). There is no prejudice to Plaintiff due to FERC’s inadvertent oversight. Plaintiff had Exhibit A for approximately three weeks prior to filing its Opposition and Cross Motion for Summary Judgment. In any event, to complete the record, FERC is filing Exhibit A herein.

standards from July 2010 through July 2019. FERC withheld the identities of certain Unidentified Registered Entities pursuant to FOIA Exemptions 3 and 7(F).

Plaintiff challenges FERC's withholdings, arguing first that FERC misapplied FOIA Exemption 3 when it concluded that the identities of violators ("Entities") were Critical Energy/Electric Infrastructure Information ("CEII" or "Critical Information") pursuant to the Fixing America's Surface Transportation Act ("FAST ACT"), 16 U.S.C. § 842o-1, and FERC's regulations. *See* Pl. Br. at 15-20.² Plaintiff next argues that FERC misapplied FOIA Exemption 7(F) when it withheld the identities of the violators who had subsequently mitigated the violations. *See* Pl. Br. at 20-39.

As discussed below, the identities of the withheld Entities are Critical Information—and exempt from FOIA pursuant to FOIA Exemption 3—because the identities, in combination with other publicly available information about the Entities' vulnerabilities, could be useful to a person in planning an attack on critical infrastructure. Thus, disclosure of the withheld Entities' identifications would reasonably pose a material risk to the bulk electric system. In addition, the identities of the withheld Entities are information compiled for law enforcement purposes the disclosure of which reasonably could be expected to endanger the life or physical safety of any individual, and thus are exempt from disclosure pursuant to FOIA Exemption 7(F). Accordingly, the Court should deny Plaintiff's motion for summary judgment and grant summary judgment in FERC's favor.

² When citing to Plaintiff's Brief, Defendant cites to the pagination generated by the Court's ECF system.

ARGUMENT

I. FERC PROPERLY APPLIED FOIA EXEMPTION 3.

A. FAST Act Section 215A is a Non-Disclosure Statute.

In 2015, Congress amended the Federal Power Act to add section 215A, authorizing the FERC and the Secretary of the Department of Energy (“Energy Secretary”) to designate information as Critical Information. *See* Fixing America's Surface Transportation Act (the “FAST Act”), 16 U.S.C. § 824o-1. Section 215A defines Critical Information as:

[I]nformation related to critical electric infrastructure, or proposed critical electrical infrastructure, generated by or provided to the 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 of the Department of Energy pursuant to subsection (d). Such term includes information that qualifies as critical energy infrastructure information under the Commission’s regulations. Critical Electric Infrastructure Information is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552, pursuant to section 215A(d)(1)(A) of the Federal Power Act.

16 U.S.C. § 824o-1(a)(2). Critical Information is exempt from disclosure under the FOIA and is not to be “made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision or tribal law requiring public disclosure of information or records.” 16 U.S.C. § 824o-1(d)(1). Thus, Section 215A is a non-disclosure statute.

Exemption 3 allows the withholding of information prohibited from disclosure by another statute if one of two disjunctive requirements are met: the statute either “(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.” *See* 5 U.S.C. § 552(B)(3)(A).³ Here, Section 215A unequivocally requires that Critical

³ 5 U.S.C. § 552(B)(3)(B) also includes statutes which “if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.” However, Section 215A does not.

Information “is exempt from mandatory disclosure” without any discretion. 5 U.S.C. § 552(B)(3)(A)(i). In fact, the D.C. Circuit has emphatically observed that Critical Information “is exempt from disclosure under [FOIA] and is not to be ‘made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision or tribal law requiring public disclosure of information or records.’” *See Union of Concerned Scientists v. Dep’t of Energy*, 998 F.3d 926, 927 (D.C. Cir. 2021) (quoting 16 U.S.C. § 824o-1(d)(1)). Accordingly, the Court should affirm FERC’s invocation of Exemption 3 to withheld CEII in this case.

B. FERC properly designated Entity Identities as Critical Information.

Once an agency establishes that a statute is a nondisclosure statute and that it meets at least one of the disjunctive requirements of Exemption 3, an agency next must establish that the records in question fall within the withholding provision of the nondisclosure statute.

Plaintiff argues that FERC was wrong when it concluded that the identities of violators were Critical Information pursuant to the FAST ACT, 16 U.S.C. § 842o-1, and FERC’s regulations. *See* Pl. Br. at 15-20. Plaintiff’s argument is premised on the absence of an official designation of the names as Critical Information pursuant to 18 C.F.R. § 388.113(c)(1). *Id.* at 16. However, plaintiff’s reading of the regulation is incomplete. Specifically, 18 C.F.R. § 388.113(c) provides:

(c) Definitions. For purposes of this section:

(1) Critical electric infrastructure information means information related to critical electric infrastructure, or proposed critical electrical infrastructure, generated by or provided to the 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 of the Department of Energy pursuant to section 215A(d) of the Federal Power Act. *Such term includes information that qualifies as critical energy infrastructure information under the Commission’s regulations.* Critical Electric Infrastructure Information is exempt from mandatory

disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3) and shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision or tribal law requiring public disclosure of information or records pursuant to section 215A(d)(1)(A) and (B) of the Federal Power Act.

18 C.F.R. § 388.113(c) (emphasis added).⁴ Thus, by definition, Critical Information need not be designated as such if it is “information that qualifies as critical energy infrastructure information under the Commission’s regulations.”

Pursuant to Congress’ direction within the FAST Act, *see* 16 U.S.C § 824o-1(d)(2), 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 Information. In amending its regulations, FERC adopted Congress’ own definition of “Critical Electric Infrastructure Information.”⁵ FERC’s regulations define “Critical Energy Infrastructure Information” as:

(2) Critical energy infrastructure information means 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;

⁴ *See also* 16 U.S.C. § 824o-1(a)(3):

The term “critical electric infrastructure information” . . . includes information that qualifies as critical energy infrastructure information under the Commission’s regulations.

⁵ Notably, both the FAST Act, as well as the Commission’s amended regulations define “critical infrastructure” in an identical manner 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.

See 16 U.S.C § 824o-1(a)(2); 18 C.F.R. § 388.113(c)(3).

- (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(c)(2).⁶ Pursuant to this regulation, information is Critical Information if it is information that “could be useful to a person in planning an attack on critical infrastructure.”

Here, plaintiff’s FOIA requests sought the disclosure of the identities of approximately 1,500 Entities and their actual or potential non-compliance with cyber-security Critical Infrastructure Protection Reliability Standards that pertain to cyber security or physical security of the nation’s electric grid.⁷ These Entities were associated with over 253 Notices of Penalty public administrative proceedings identified by separate FERC docket numbers.⁸ The public version of a Critical Infrastructure Protection—related Notices of Penalty do 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. *See* Declaration of Barry W. Kuehnle, ECF No. 41-2 (“Kuehnle Decl.”) ¶ 10. The non-public Notices of Penalties contain the names of Entities found to have violated Critical

⁶ FERC also uses the term Critical Information to collectively refer to both definitions. *See* Order 833, Regulations Implementing FAST Act Section 61003—Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information; Availability of Certain North American Electric Reliability Corporation Databases to the Commission, 157 FERC ¶ 61,123, P 9 (Nov. 17, 2016).

⁷ The North American Reliability Corporation is the FERC-designated Electric Reliability Organization responsible for the development and enforcement, subject to FERC review, of Critical Infrastructure Protection Reliability Standards. *See* Kuehnle Decl. ¶ 8.

⁸ For ease of reference, the “Find, Fix, and Track Report,” the Spreadsheet Notice of Penalty,” and the “Notice of Penalty” are referred to collectively herein as a “Notice of Penalty.” *See also* Kuehnle Decl. ¶ 7, n.1.

Infrastructure Protection-related Reliability Standards as well as additional details regarding the nature of the relevant violation. *Id.*

Thus, the disclosure of an Entities' identity, when combined with public information about the Entities' vulnerabilities set out in the publicly available Notices of Penalty, would be useful to those seeking to target the nation's electric grid. Kuehnle Decl. ¶¶ 12, 17–18.⁹ 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. This remains true even if the violation has been mitigated because even though mitigated, the type of violation shows the type of vulnerability.¹⁰

Importantly, Plaintiff is not seeking only the identities of Entities, but rather, he is seeking identities of Entities that can be examined in concert with other details surrounding their 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's name was appropriate involved an examination of information that is already publicly available within the public Notice of Penalty. *Id.* ¶ 14.

⁹ As to a violation of cyber security standards, even if mitigated, would create a risk of harm or detriment to life, physical safety, or security of the public because such violations directly bear on 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. *See* Complaint, ECF No. 1, ¶¶ 3- 14.

¹⁰ Using plaintiff's analogy of the locked gate, Pl. Br. at 21, knowing which person's gate had been left unlocked is useful because the gate-owner's carelessness may reasonably reoccur regardless of whether he re-locked the gate one time. *See also* Pl. Br. at 30-31 (attempting to distinguish the records created to protect dams from terrorists at issue in *Living Rivers, Inc. v. U.S. Bureau of Reclamation*, 272 F. Supp. 1313 (D. Utah 2003), from the records created to protect the nation's electric grid from attack here).

FERC conducted a case-by-case assessment of the requested information included an analysis 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:

1. the nature of the Critical Infrastructure Protection Reliability Standard violation, including whether there is a Technical Feasibility Exception involved that does not allow the Entity to fully meet the standards;
2. whether vendor-related information is contained in the Notices of Penalty;
3. whether mitigation is complete;
4. the extent to which the disclosure of the identity of the Entity and other information would be useful to someone seeking to cause harm;
5. whether a successful audit has occurred since the violation(s);
6. whether the violation(s) was administrative or technical in nature; and
7. the length of time that has elapsed since the filing of the public Notice of Penalty.

See Kuehnle Decl. ¶¶ 13-14, Ex. A. Accordingly, because the Entities' identities constituted Critical Information it is exempt from disclosure pursuant to FOIA Exemption 3.¹¹

II. FERC PROPERLY APPLIED FOIA EXEMPTION 7(F).

Not only are the Entities' identities Critical Information, they are also exempt from disclosure because the Entities' identities also constitute "law enforcement information," the disclosure of which could reasonably be expected to endanger the life or physical safety of any individual (those connected to the impacted portion of the power grid impaired by an attack). Plaintiff does not contest that these "records or information [were] compiled for law enforcement purposes. Plaintiff disputes whether these documents could reasonably be expected to endanger the life or physical safety of any individual. *See* Pl. Br. at 21-31.

¹¹ As amended, Exemption 3 allows the withholding of information prohibited from disclosure by another statute only if one of two disjunctive requirements are met: the statute either "(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld." *See* 5 U.S.C. § 552(B)(3)(A). A statute thus falls within the exemption's coverage if it satisfies any one of its disjunctive requirements.

For the same reasons set forth in the Kuehnle Declaration relating to classifying the Entities' identities as Critical Information—specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that could be useful to a person in planning an attack on critical infrastructure, *see* 18 C.F.R. § 388.113(c)(2)(ii)—the release and use of these documents could reasonably be expected to endanger the life or physical safety of any individual. Kuehnle Decl. ¶ 17. In other words, the knowledge about an Entities' cyber security vulnerability, even if mitigated, creates a very real target for those intent on hacking into the system. Were the computers and networks comprising the industrial control system of an Entity hacked, it could leave the system inoperable. *Id.* Such a cyberattack of the electric grid system and the distribution of electricity undeniably could reasonably be expected to endanger the life and physical safety of those people whose power has been cut off. *Id.* Further, FERC's assessment of danger, in applying Exemption 7(F), should be 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.”); *see also 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.”). Thus, FERC's application of FOIA Exemption 7(F) is fully supported by the Keunle Declaration and is appropriate.

III. FERC MET ITS BURDEN OF PROOF.

Plaintiff argues that FERC failed to present a *Vaughn* index and thus FERC failed provide a sufficient description of the withheld or redacted documents and the bases for those

withholdings.¹² Pl. Br. at 9-11. Plaintiff's argument lacks merit because it elevates form over substance. Under FOIA jurisprudence, the government need not always justify its withholdings via a *Vaughn* index or on a document-by-document basis and can, through reasonably detailed affidavits, meet its burden of proof by categorical showings. *See Tax Analysts v. IRS*, 414 F. Supp. 2d 1, 4 (D.D.C. 2006) (collecting cases); *see also Gallant v. NLRB*, 26 F.3d 168, 173 (D.C. Cir. 1994) (holding that "production of a *Vaughn* Index was not necessary given the adequacy of the government's affidavits."). An agency may submit materials in any form, including an affidavit or oral testimony, so long as they give the reviewing court a reasonable basis to evaluate the claim of privilege. *Id.* (cleaned up).

Here, the Kuehnle Declaration affords the Court fully adequate grounds to determine the appropriateness of the Critical Information designation and the law enforcement exemption. A traditional *Vaughn* index would not illuminate the Court on the issues at hand—whether the Entities' identities are indeed Critical Information pursuant to statutory and regulatory provisions and whether disclosing the Entities' identities could reasonably be expected to endanger life or physical safety of any individual. Because all records requested by plaintiff under FOIA fall under both FOIA Exemptions and 7(F), an index would be extremely repetitive, would provide no useful additional information beyond that contained in the detailed Kuehnle Declaration, and would therefore serve no real purpose. A *Vaughn* index will not assist the Court in determining whether the advisory documents sought fall under the statute or alternately are protected by the law enforcement exemption.

¹² *Vaughn v. Rosen*, 484 F.2d 820, 826 (D.D.C. 1973).

CONCLUSION

For the foregoing reasons, the Court should deny Plaintiff's motion for summary judgment and grant summary judgment in FERC's favor.

Dated: August 10, 2022

Respectfully submitted,

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

BRIAN P. HUDAK,
Chief, Civil Division

/s/ T Anthony Quinn
T. ANTHONY QUINN
D.C. Bar No. 415213
Assistant United States Attorney
United States Attorney's Office
Civil Division
601 D Street, NW
Washington, D.C. 20530
Tony.Quinn2@usdoj.gov

Attorneys for Defendant

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL MABEE,

Plaintiff,

v.

FEDERAL ENERGY REGULATORY
COMMISSION,

Defendant.

Civil Action No. 19-3448 (FYP)

[PROPOSED] ORDER

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

ORDERED that the Defendant's Motion is GRANTED. It is further

ORDERED that the Plaintiff's Cross-Motion for Summary Judgment is DENIED. It is further

ORDERED that summary judgment is entered in favor of Defendant.

Dated: _____

FLORENCE Y. PAN
United States District Judge

1. Is a cybersecurity Technical Feasibility Exception(s) associated with this NOP?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2. Are there any outstanding enforcement actions or uncompleted mitigations plans associated with this NOP?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3. Has the Entity completed a subsequent audit? Please explain below:	<input type="checkbox"/> Yes <input type="checkbox"/> 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:	<input type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No