

Michael Mabee

(516) 808-0883

CivilDefenseBook@gmail.com

June 16, 2018

James Danly, General Counsel
Federal Energy Regulatory Commission
888 First Street, NE,
Washington, D.C. 20426
Via Email: james.danly@ferc.gov

Subject: Appeal of Determination in FOIA No. FY18-75

Dear Mr. Danly:

On April 13, 2018 I submitted a FOIA request to the Federal Energy Regulatory Commission (FERC). This Request (FOIA-2018-75) is attached hereto as Exhibit A.¹ On April 23, 2018 FERC sent a letter to the North American Electric Reliability Corporation (NERC) requesting their views on the release of the information I seek. This letter is attached hereto as Exhibit B. On April 30, 2018 NERC responded. Their response is attached hereto as Exhibit C. On May 11, 2018 FERC notified me of an extension of time. This notification is attached hereto as Exhibit D. On May 25, 2018 FERC denied my FOIA request in its entirety. The denial letter is attached hereto as Exhibit E. I hereby appeal FERC's determination.

Description of records sought:

Regarding FERC Docket No. NP18-7-000:

1. I seek correspondence between FERC and the North American Electric Reliability Corporation (NERC) identifying the "Unidentified Registered Entity" described in the document: "NERC Full Notice of Penalty regarding Unidentified Registered Entity" filed with FERC on February 28, 2018.
2. I also seek any correspondence between FERC and NERC laying out any purported rationale for withholding the identity of the "Unidentified Registered Entity" from public view.

The records sought are not Critical Energy Infrastructure Information (CEII) or otherwise classified to protect national security:

I note that FERC Order No. 833 holds that the Commission's practice is that information that "simply give[s] the general location of the critical infrastructure" or simply provides the name of the facility is not Critical Energy Infrastructure Information (CEII).² I am not seeking any CEII. I simply ask for disclosure

¹ While the determination letter dated May 25, 2018 makes no reference to my fee waiver request, I assume it was granted. If the issue must be revisited for any reason, I hereby incorporate my fee waiver request of April 13, 2018 by reference.

² Order No. 833 at pg. 17. Also see 18 C.F.R. §388.113(c)(1)(iv).

of the identity of the “Unidentified Registered Entity” and why this information has been withheld. I also note that the name of the entity has been widely speculated in the media.³

There is no national security reason or FOIA exemption that should prevent disclosure of the identity of this violator of reliability standards to the public, because the NERC Notice of Penalty claims that the cybersecurity vulnerability has been remedied. I further note that the public has already been forced to wait at least 520 days before learning of the bare details of this incident, according to the NERC Notice of Penalty which states that sensitive cybersecurity information was exposed to the public internet for 70 days and the total duration of the violation was 590 days. This should have been ample time to remedy the cybersecurity violation. At this late date, the public should not be indefinitely prevented from learning the identity of the violator.

The records sought would not reveal trade secrets and commercial or financial information obtained from a person and privileged or confidential:

I note that it has been standard practice for FERC and NERC to disclose the identities of the entities who are subject to regulatory fines by NERC. Those entities violating reliability standards have not been considered privileged or confidential information.

I also note that it is inconsistent with a well-functioning democracy for monetary penalties to be assessed against regulated entities whose identities are then held as secrets. I urge the Commission to reconsider the implications of allowing NERC, the FERC-designated Electric Reliability Organization (ERO), to have delegated authority to assess fines for wrongdoing and then to keep the identities of wrongdoers from public view. I know of no other federal regulator that allows this odious practice.

The records may be provided to me electronically at this email address: CivilDefenseBook@gmail.com.

Sincerely,



Michael Mabee

Attachments

CC: Charles A. Beamon, Associate General Counsel
Via Email: charles.beamon@ferc.gov

³ Information Security Media Group. “US Power Company Fined \$2.7 Million Over Data Exposure - Grid Regulator Says Company Left Critical Data Exposed for 70 Days.” March 14, 2018. <https://www.bankinfosecurity.com/us-power-company-fined-27-million-over-data-exposure-a-10715> (accessed March 24, 2018); Gizmodo Media Group. “US Power Company Fined \$2.7 Million Over Security Flaws Impacting 'Critical Assets'.” March 13, 2018. <https://gizmodo.com/us-power-company-fined-2-7-million-over-security-flaws-1823745994> (accessed March 17, 2018).

Michael Mabee

(516) 808-0883

CivilDefenseBook@gmail.com

FOIA-2018-75

Accepted: April 13, 2018

Track 2

Due Date: May 11, 2018

April 13, 2018

Leonard Tao,
Director and Chief FOIA Officer
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Subject: Request under the Freedom of Information Act (FOIA), 5 U.S.C. § 552.

Dear Mr. Tao:

I request records under the Freedom of Information Act, which are described below. Further, as more fully set forth below, I also request a fee waiver as I have no commercial interest in the described records and it is in the public interest for the Federal Energy Regulatory Commission (FERC) to disclose these records to the public.

Description of records sought:

Regarding FERC Docket No. NP18-7-000:

1. I seek correspondence between FERC and the North American Electric Reliability Corporation (NERC) identifying the "Unidentified Registered Entity" described in the document: "NERC Full Notice of Penalty regarding Unidentified Registered Entity" filed with FERC on February 28, 2018.
2. I also seek any correspondence between FERC and NERC laying out any purported rationale for withholding the identity of the "Unidentified Registered Entity" from public view.

The records sought are not Critical Energy Infrastructure Information (CEII) or otherwise classified to protect national security:

I note that FERC Order No. 833 holds that the Commission's practice is that information that "simply give[s] the general location of the critical infrastructure" or simply provides the name of the facility is not Critical Energy Infrastructure Information (CEII).¹ I am not seeking any CEII. I simply ask for disclosure of the identity of the "Unidentified Registered Entity" and why this information has been withheld. I also note that the name of the entity has been widely speculated in the media.²

¹ Order No. 833 at pg. 17. Also see 18 C.F.R. §388.113(c)(1)(iv).

² Information Security Media Group. "US Power Company Fined \$2.7 Million Over Data Exposure - Grid Regulator Says Company Left Critical Data Exposed for 70 Days." March 14, 2018. <https://www.bankinfosecurity.com/us-power-company-fined-27-million-over-data-exposure-a-10715> (accessed March 24, 2018); Gizmodo Media Group. "US Power Company Fined \$2.7 Million Over Security Flaws Impacting 'Critical Assets'." March 13, 2018. <https://gizmodo.com/us-power-company-fined-2-7-million-over-security-flaws-1823745994> (accessed March 17, 2018).

There is no national security reason or FOIA exemption that should prevent disclosure of the identity of this violator of reliability standards to the public, because the NERC Notice of Penalty claims that the cybersecurity vulnerability has been remedied. I further note that the public has already been forced to wait at least 520 days before learning of the bare details of this incident, according to the NERC Notice of Penalty which states that sensitive cybersecurity information was exposed to the public internet for 70 days and the total duration of the violation was 590 days. This should have been ample time to remedy the cybersecurity violation. At this late date, the public should not be indefinitely prevented from learning the identity of the violator.

The records sought would not reveal trade secrets and commercial or financial information obtained from a person and privileged or confidential:

I note that it has been standard practice for FERC and NERC to disclose the identities of the entities who are subject to regulatory fines by NERC. Those entities violating reliability standards have not been considered privileged or confidential information.

I also note that it is inconsistent with a well-functioning democracy for monetary penalties to be assessed against regulated entities whose identities are then held as secrets. I urge the Commission to reconsider the implications of allowing NERC, the FERC-designated Electric Reliability Organization (ERO), to have delegated authority to assess fines for wrongdoing and then to keep the identities of wrongdoers from public view. I know of no other federal regulator that allows this odious practice.

Request for Waiver of Fees:

I am a private citizen with expertise in emergency preparedness and critical infrastructure protection. I maintain a blog where I intend to disseminate this information³. I accept no advertising on my blog and derive no revenue from writing or posting my blog articles.

As set forth fully below, I am entitled to a waiver of fees as I meet all the requirements of 18 C.F.R. §388.109(c).

Requirement: In accordance with 18 C.F.R. §388.109(c)(1), "(1) Any fee described in this section may be reduced or waived if the requester demonstrates that disclosure of the information sought is: (i) In the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government, and (ii) Not primarily in the commercial interest of the requester."

Answer: Disclosure of this information will inform the public as to the actions the government and the designated ERO have taken to insure the security of the bulk power system. There has been a great deal of media attention and government notices regarding recent cyberattacks and cybersecurity breaches to the electric grid.⁴ Disclosure of the requested information is critical to the public's understanding of how

³ <https://michaelmabee.info/category/mikes-blog/> (accessed April 13, 2018).

⁴ See for example: US-CERT Alert (TA18-074A) <https://www.us-cert.gov/ncas/alerts/TA18-074A> (accessed March 15, 2018); Gizmodo: "FBI and DHS Warn That Russia Has Been Poking at Our Energy Grid." <https://apple.news/AHv5RwYqbSf-El-yIa355Jw> (accessed March 15, 2018); Washington Free Beacon: "Russia Implicated in Ongoing Hack on U.S. Grid." <https://apple.news/AGs6ieh6wSP-1tQkUFttREA> (accessed March 15, 2018); Slate: "What Does It Mean to Hack an Electrical Grid?" <https://apple.news/Au5gy7bTITDSovpvzg5j79w>

FERC and the ERO holds regulated entities accountable to compliance with regulatory standards for cybersecurity.

I have no commercial interest in these records and will use these records in research and information dissemination to the public.

Requirement: In accordance with 18 C.F.R. §388.109(c)(2) “The Commission will consider the following criteria to determine the public interest standard:”

Answer: I will answer each criterion in turn.

Criterion: (i) “Whether the subject of the requested records concerns the operations or activities of the government”

Answer: The protection of the critical infrastructure, including the bulk power system, is a clear function of the federal government.⁵ The regulation of the critical infrastructures by the federal government and the transparency of the process – including the identities of entities that violate reliability standards– concerns the operations or activities of the government.

Criterion: (ii) “Whether the disclosure is likely to contribute to an understanding of government operations or activities”

Answer: According to NERC, ““These violations posed a serious or substantial risk to the reliability of the bulk power system (BPS).” The entity in question risked the reliable operation of the bulk power system and therefore the public has a right to examine this incident and the behavior and actions of the violating entity.

Criterion: (iii) “Whether disclosure of the requested information will contribute to public understanding”

Answer: As previously noted, there has been a great deal of public attention, press articles and increased awareness to the threat of cyberattacks against the bulk power system. The identity of entities that place the public at risk by violating cybersecurity standards is critical to the public understanding of the effectiveness of existing standards.

Criterion: (iv) “Whether the disclosure is likely to contribute significantly to public understanding of government operations or facilities.”

Answer: Under Section 215 of the Federal Power Act, regulation of the bulk power system is clearly a government operation. The public needs to understand how reliability standards are being enforced.

Requirement: In accordance with 18 C.F.R. §388.109(c)(3) “The Commission will consider the following criteria to determine the commercial interest of the requester:”

⁵ Executive Order 13800 “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.” May 11, 2017. <https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf> (accessed March 24, 2018); Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience. February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (accessed March 24, 2018).

Answer: I will answer each criterion in turn.

Criterion: (i) Whether the requester has a commercial interest that would be furthered by the requested disclosure.

Answer: No. The requester a private citizen and has no commercial interest in the information.

And, if so: criterion: (ii) Whether the magnitude of the identified commercial interest of the requester is sufficiently large, in comparison with the public interest in disclosure, that disclosure is primarily in the commercial interest of the requester.

Answer: Not applicable since the requester has no commercial interest in the information.

The records may be provided to me electronically at this email address: CivilDefenseBook@gmail.com.

Sincerely,

A handwritten signature in blue ink, appearing to read "MK", is positioned above the name Michael Mabee.

Michael Mabee

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

APR 23 2018

Re: Submitter's Rights Letter,
FOIA No. FY18-075

VIA E-MAIL AND REGULAR MAIL

Edwin G. Kichline
Senior Counsel and Director of
Enforcement Oversight
North American Electric Reliability Corporation
1325 G Street N.W. Suite 600
Washington, DC 20005
edwin.kichline@nerc.net

Dear Mr. Kichline:

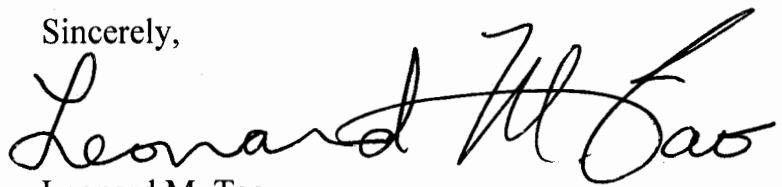
Pursuant to the Freedom of Information Act (FOIA)¹ and the Federal Energy Regulatory Commission's (Commission) regulations, 18 C.F.R. § 388.112(d) (2017), you are hereby notified that an individual has filed a request seeking to obtain correspondence between FERC and NERC identifying the "Unidentified Registered Entity" as described in the "NERC Full Notice of Penalty regarding Unidentified Registered Entity" filed February 28, 2018 in docket NP18-7. He is also seeking correspondence between FERC and NERC laying out the rationale for withholding the identity of the "Unidentified Registered Entity".

Because your company has asserted a privileged and confidential interest in the information requested, we are soliciting your comments on whether release of the information is required under the FOIA. Your written comments are due within five business days from the date of this letter, and should clearly explain whether you oppose the release of this document, or portions thereof, and the rationale for your position. The Commission will not be persuaded by conclusory statements as to why the information deserves protection. The Commission may construe a non-response as evidence that you do not object to releasing the document.

Your comments, if any, may be mailed to the undersigned at the Federal Energy Regulatory Commission, 888 First Street, NE, Washington, D.C. 20426. Your comments may also be mailed electronically to the email address provided below or sent via facsimile to (202) 208-2106. If you have any questions regarding this matter, please contact Ms. Toyia Johnson of my staff by phone at (202) 502-6088 or e-mail to foia-ceii@ferc.gov.

¹ 5 U.S.C. § 552, *as amended* by the FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 (2016).

Sincerely,

A handwritten signature in black ink that reads "Leonard M. Tao". The signature is written in a cursive style with a large, sweeping "L" and "T".

Leonard M. Tao
Director
Office of External Affairs

cc: Michael Mabee

A black rectangular redaction box covering the name of the second recipient.

CivilDefenseBook@gmail.com

April 30, 2018

VIA ELECTRONIC SUBMISSION

Mr. Leonard M. Tao
Director
Office of External Affairs
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Response to FOIA-2018-75 (Docket No. NP18-7-000)

Dear Ms. Bose:

The North American Electric Reliability Corporation (“NERC”) hereby objects to release of the identity of the Unidentified Registered Entity (“URE”) subject to the NERC Notice of Penalty filed in Docket No. NP18-7-000, as sought in Freedom of Information Act (“FOIA”) Request FOIA-2018-75.

NERC is compelled to object to this FOIA Request, because the Federal Energy Regulatory Commission (“Commission”) has instructed NERC not to divulge the identity of entities that have violated NERC Critical Infrastructure Protection (“CIP”) Reliability Standards. The Commission’s expectation that NERC should not identify entities violating CIP Reliability Standards is longstanding but is most recently reflected in FERC’s 2014 *Order on the Electric Reliability Organization’s Five-Year Performance Assessment*. In that order, the Commission stated that, “[w]ith respect to concerns and questions raised regarding NERC’s protection of information deemed to be confidential, particularly as related to cybersecurity incidents or CIP violations, we believe that NERC currently has adequate rules and procedures in place to protect against improper disclosure of sensitive information (...).” *Order on the Electric Reliability Organization’s Five-Year Performance Assessment*, 149 FERC ¶ 61,141, at n. 55, P 47, and n. 65 (2014) (in response to a commenter referencing a prior inadvertent disclosure of the identity of a URE sanctioned for violations of CIP Reliability Standards).

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline

*Senior Counsel and Director of Enforcement
Oversight*

North American Electric Reliability Corporation

cc. Ms. Toyia Johnson, FERC

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

May 11, 2018

Re: Extension of Time, Freedom of
Information Act Request, FOIA
No. FY18-75

VIA E-MAIL AND REGULAR MAIL

Michael Mabee



CivilDefenseBook@gmail.com

Dear Mr. Mabee:

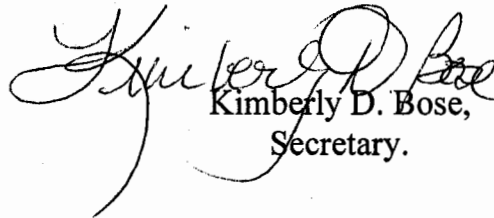
This letter is in reference to your Freedom of Information Act, 5 U.S.C. § 552 (2006), *as amended by* OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524, request filed with the Federal Energy Regulatory Commission (Commission) on March 13, 2018. We have determined that to reply to your request, we need to consult with other components of the agency having substantial subject-matter interest therein. *See* 18 C.F.R. § 388.110(b)(1) and (b)(4)(iii) (2017).

Therefore, in accordance with the provisions in Section 388.110(b) of the Commission's Rules of Practice and Procedure, we are notifying you that we have extended the time limit to make an initial determination on your request. We expect to be able to send you an initial determination on your request by May 25, 2018.

You have the right to seek dispute resolution services from the FOIA Public Liaison of the agency or the Office of Government Information Services (OGIS). Using OGIS services does not affect your right to pursue your appeal. You may contact OGIS by mail

at Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, MD 20740-6001; email at ogis@nara.gov; telephone at (301) 837-1996; facsimile at (301) 837-0348; or toll-free at 1-877-684-6448.

Cordially,



Kimberly D. Bose,
Secretary.

cc: Leonard M. Tao
Director
Office of External Affairs
Federal Energy Regulatory Commission
Washington, D.C. 20426

Federal Energy Regulatory Commission
Washington, DC 20426

MAY 25 2018

Re: FOIA No. FY18-75
Response

VIA E-MAIL AND REGULAR MAIL

Michael Mabee

[REDACTED]

[REDACTED]

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

This is a response to your correspondence received on April 13, 2018, in which you requested information pursuant to the Freedom of Information Act (FOIA)¹, and the Federal Energy Regulatory Commission's (Commission) FOIA regulations, 18 C.F.R. § 388.108. Specifically, you requested a copy of the following:

1. I seek correspondence between FERC and the North American Electric Reliability Corporation (NERC) identifying the 'Unidentified Registered Entity' described in the document: 'NERC Full Notice of Penalty regarding Unidentified Registered Entity' filed with FERC on February 28, 2018.
2. I also seek any correspondence between FERC and NERC laying out any purported rationale for withholding the entity of the 'Unidentified Registered Entity' from public view.

On April 23, 2018, Commission staff notified NERC of your request and provided an opportunity to comment pursuant to 18 C.F.R. § 388.112. NERC submitted comments on April 30, 2018, objecting to "the FOIA Request because [FERC] has instructed NERC not to divulge the identity of entities that have violated NERC Critical Infrastructure Protection ('CIP') Reliability Standards." In support of the foregoing, NERC cites various Commission orders.

¹ 5 U.S.C. § 552, *as amended* by the FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 (2016).

A search of the Commission's non-public records has identified approximately seven (7) responsive documents² that are responsive to your request(s), consisting of various email correspondence between FERC and NERC regarding questions concerning details relative to the incident resulting in the Notice of Penalty. Such questions include detailed discussions of mitigation efforts and risk analysis, as well as the Unidentified Registered Entity's Cyber Security Incident Response Plan(s). As explained below, the documents are protected from disclosure pursuant to FOIA Exemptions 3 and 7, and therefore will not be released.

Exemption 3

The documents are designated as CEII and thus, exempt from mandatory disclosure pursuant to FOIA Exemption 3.³

Exemption 7(F)

The requested documents, including the identity of the Unidentified Registered Entity, are also exempt from mandatory disclosure under FOIA Exemption 7(F), which exempts "records or information compiled for law enforcement purposes" to the extent that release of such information "could reasonably be expected to endanger the life or physical safety of any individual." See 5 U.S.C. § 552(b)(7)(F). The requested material contains information regarding cyber security and risks to the Unidentified Registered Entity, as well the techniques used to resolve the incident and associated possible vulnerabilities. I also note that 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. Accordingly, the requested material is being withheld under FOIA Exemption 7(F).

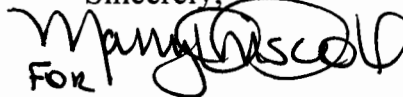
² Please note that Commission staff searched for responsive documents available through the date in which your FOIA request was accepted by the Commission, April 13, 2018.

³ CEII is specifically exempted from disclosure under the Fixing America's Surface Transportation Act, Pub. L. No. 118-94, § 61003 (2015) (establishing applicability of FOIA Exemption 3, 5 U.S.C. 552(b)(3) (protecting material specifically exempted by statute).

As provided by FOIA, any appeal from this determination must be filed within 90 days of the date of this letter. The appeal must be in writing, addressed to James Danly, General Counsel, Federal Energy Regulatory Commission, 888 First Street, NE, Washington, D.C. 20426, and clearly marked "Freedom of Information Act Appeal." Please include a copy to Charles A. Beamon, Associate General Counsel, General and Administrative Law, at the same address.

You also have the right to seek dispute resolution services from the FOIA Public Liaison of the agency or the Office of Government Information Services (OGIS). Using OGIS services does not affect your right to pursue your appeal. You may contact OGIS by mail at Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, MD 20740-6001; email at ogis@nara.gov; telephone at 301-837-1996; facsimile at 301-837-0348; or toll-free at 1-877-684-6448.

Sincerely,

A handwritten signature in black ink, appearing to read "Leonard Tao", written over a circular stamp or seal.

For

Leonard Tao

Director

Office of External Affairs