

Michael Mabee



(516) 808-0883

CivilDefenseBook@gmail.com

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 "ML", is placed on a light yellow rectangular background.

Michael Mabee