UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NERC Full Notice of Penalty regarding	**)**	
Unidentified Registered Entity	**)**	**Docket No. NP18-7-000**
	)	

REQUEST TO INTERVENE

Submitted to FERC on April 15, 2018

Michael Mabee, a private citizen, requests the Commission's leave to intervene in the above captioned docket, pursuant to 18 C.F.R. § 39.7(e)(4)[1]. My proposed intervention is limited to requesting that the Commission review this Notice of Penalty to insure that it is in the public interest. Based on the limited public information available, this Notice of Penalty raises several significant public interest concerns.

Background on the Intervenor

I am a private citizen with expertise on emergency preparedness, specifically on community preparedness for a long-term power outage. My career includes experience as an urban emergency medical technician and paramedic, a suburban police officer, and in the federal civil service. In the U.S. Army, I served in two wartime deployments to Iraq and two humanitarian missions to Guatemala. I retired from the U.S. Army Reserve in 2006 at the rank of Command Sergeant Major (CSM). I was decorated by both the U.S. Army and the federal government for my actions on 9/11/2001 at the World Trade Center in New York City. In sum, I have a great deal of experience – both overseas and in the U.S. – working in worlds where things went wrong. I have studied the vulnerabilities of the U.S. electric grid to a variety of threats. My research lead me to write two books about how communities can prepare for and survive a long term power outage.[2] I continue to write extensively on emergency preparedness for blackout.

Background on FERC Docket No. NP18-7-000

On February 28, 2018 NERC issued a "Notice of Penalty regarding Unidentified Registered Entity"[3] in which the NERC-anonymized entity apparently agreed to pay penalties of $2,700,000 for two very serious violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards. According to NERC, this data breech involved "30,000 asset records, including records associated with Critical Cyber Assets (CCAs). The records included information such as IP addresses and server host names."

According to NERC

> "These violations posed a serious or substantial risk to the reliability of the bulk power system (BPS). The CCAs associated with the data exposure include servers that store user data, systems that control access within URE's control centers and substations, and a supervisory control and data acquisition (SCADA) system that stores critical CCA Information. The data was exposed publicly on the Internet for 70 days. The usernames of the database were also exposed, which included cryptographic information of those usernames and passwords.

> Exposure of the username and cryptographic information could aid a malicious attacker in using this information to decode the passwords. This exposed information increases the risk of a malicious attacker gaining both physical and remote access to URE's systems. A malicious attacker could use this information to breach the secure infrastructure and access the internal CCAs by jumping from host to host within the network. Once in the network, the attacker could attempt to login to CCAs, aided by the possession of username and password information."

Concerns Raised by the Publically Available Information Which Should Trigger Commission Review

1. Prompt reporting requirement: It is unclear from the publically available information whether the Electric Reliability Organization (North American Electric Reliability Corporation) or the Regional Entity (Western Electricity Coordinating Council) "report[ed] promptly to the Commission any self-reported violation or investigation of a violation or an alleged violation of a Reliability Standard" in accordance with 18 CFR § 39.7(b). The Commission should determine whether this requirement was satisfactorily met.

2. Identity of the "Unidentified Registered Entity." NERC's lack of transparency by hiding the identity of the "Unidentified Registered Entity" from the public is against the public interest and should not be allowed by the Commission.

    a. At the time the matter was filed with the Commission, the name should have been disclosed publically. 18 CFR § 39.7(b)(4) states that: "Each violation or alleged violation shall be treated as nonpublic until the matter is filed with the Commission as a notice of penalty or resolved by an admission that the user, owner or operator of the Bulk-Power System violated a Reliability Standard or by a settlement or other negotiated disposition." [Emphasis added.] Therefore, when NERC filed their notice of penalty on February 28, 2018, the name of the entity should have been disclosed publically.
    b. The notice of penalty is defective. In accordance with 18 CFR § 39.7(d)(1), the notice of penalty must include "[t]he name of the entity on whom the penalty is imposed."
    c. NERC cannot argue that the name of the entity is Critical Energy Infrastructure Information (CEII). 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).[4] We also note that the name of the entity has been widely speculated in the media.[5] NERC withholding the name of the entity is against the public interest.
    d. NERC cannot argue that this should be a non-public proceeding related to a "cybersecurity incident"[6] as this does not meet the regulatory definition of a "cybersecurity incident."[7] According to NERC, this incident was a not "malicious act" as the definition of "cybersecurity incident" requires – rather it was a colossal blunder on the part of the regulated entity. The public has the right to know who endangered them.

3. The terms of the settlement agreement are suspicious and should be reviewed by the commission to insure that they are fair and in the public interest. The relatively light penalty and non-admission clause raise immediate concerns. If the Western Electricity Coordinating Council truly concluded, as NERC states, that two violations of the Critical Infrastructure Protection (CIP) Reliability Standards were committed, why is the entity being allowed to enter an agreement where it "neither admits nor denies the violations"? Such an agreement is against the public interest as it does not serve as a

deterrent for future violations in the industry. What strong incentive is there for regulated entities to adhere to Critical Infrastructure Protection (CIP) Reliability Standards if the penalties are light, they do not have to admit fault for violations, and their identity will not be disclosed.

4. The settlement agreement should be released to the public. The terms of the agreement are only vaguely discussed in the notice of penalty and therefore should be available for public scrutiny. There could be terms that are contrary to the public interest (such as any form of confidentiality clause).

Conclusion:

For the forgoing reasons, I request that the Commission fully review the notice of penalty and the surrounding circumstances to insure that the resolution is in the public interest and that the identity of the "Unidentified Registered Entity" is promptly disclosed to the public.

Respectfully submitted by:

Michael Mabee

---

[1] On March 30, 2018, the Commission extended until May 29, 2018, the time period for consideration whether to review on its own motion the penalty contained in the Notice of Penalty in Docket No. NP18-7-000. 162 FERC ¶ 61,291.

[2] Mabee, Michael. *The Civil Defense Book: Emergency Preparedness for a Rural or Suburban Community*. ISBN-13: 978-1974320943, first edition published July 4, 2013, second edition published October 17, 2017.

[3] NERC "Full Notice of Penalty regarding Unidentified Registered Entity FERC Docket No. NP18-_-000." February 28, 2018. http://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_NOC-2569%20Full%20NOP.pdf (accessed April 7, 2018).

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

[5] 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 April 7, 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 April 7, 2018).

[6] 18 CFR § 39.7(e)(7)

[7] 18 CFR § 39.1 defines "cybersecurity incident" as "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the Reliable Operation of the Bulk-Power System."

Document Content(s)