

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

**Petition for Rulemaking to Require Disclosure )  
of Names of Regulated Entities Subject to )  
Regulatory Actions by the Commission or )  
by the Electric Reliability Organization )  
)  
Michael Mabee, Petitioner )**

Docket No. \_\_\_\_\_

Submitted to FERC on February 5, 2019

Pursuant to 18 CFR § 385.207 (Rule 207), the petitioner respectfully submits this request for rulemaking for a declaratory order or rule “to terminate a controversy or remove uncertainty”<sup>1</sup> or, in the alternative, a rule of general applicability,<sup>2</sup> consistent with Commission authority for electric reliability under Section 215 of the Federal Power Act.<sup>3</sup> I ask that the Federal Energy Regulatory Commission (“FERC” or “the Commission”) order that the identities of regulated entities subject to regulatory actions by the Commission or by the Electric Reliability Organization (“ERO”) shall be publicly disclosed. Disclosure of the identities of utility violators and their settlement agreements is vital to ensure the reliability of the electric grid and the national security of the United States. If FERC allows the names of utilities who violate physical and cybersecurity standards to be hidden, there will be poor incentives for security improvements. A foreign attack on the electric grid could result in a long-term blackout, causing millions of Americans to die from disease and starvation.

**Introduction**

“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.”

– Justice Louis D. Brandeis

---

<sup>1</sup> 18 CFR § 385.207(a)(2)

<sup>2</sup> 18 CFR § 385.207(a)(4)

<sup>3</sup> 16 U.S.C. § 824o.

In an official assessment to the U.S. Congress released on January 29, 2019, the U.S. Intelligence Community confirmed that the U.S. electric grid is not secure against foreign incursions:<sup>4</sup>

Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.

Vulnerability of the U.S. electric grid to foreign attack has been longstanding. In an April 8, 2009 article, “Electricity Grid in U.S. Penetrated By Spies,” the *Wall Street Journal* disclosed:<sup>5</sup>

Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.

"The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."

FERC's decade-long failure to secure the U.S. electric grid is in large part due to its complicity in a North American Electric Reliability Corporation (NERC) enforcement regime that shields the identities of standard violators from outside scrutiny. The NERC coverup, enabled and abetted by FERC, started in July 2010. (Previous to July 10, 2010, identities of standards violators were disclosed by both NERC and FERC.) Under this apparently illegal enforcement regime, incentives for electric utilities have become clear: devote only moderate attention to grid security while knowing any gaps will be kept hidden from ratepayers, the U.S. Congress, and the public at

---

<sup>4</sup> Coats, Daniel R. “Worldwide Threat Assessment of the U.S. Intelligence Community” Senate Select Committee on Intelligence. January 29, 2019. <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf> (accessed February 5, 2019).

<sup>5</sup> Gorman, Siobhan. “Electricity Grid in U.S. Penetrated By Spies.” *Wall Street Journal*. April 8, 2009. <https://www.wsj.com/articles/SB123914805204099085> (accessed February 5, 2019).

large. In its consideration of this Petition, FERC now has the opportunity to end these practices injurious to national security and the public interest.

Disclosure is the cornerstone of a successful regulatory scheme in a free society. The Securities and Exchange Commission routinely publicizes the names of companies and individuals subject to regulatory actions under U.S. securities laws;<sup>6</sup> the Food and Drug Administration routinely publicizes the names of companies whose food is being recalled due to public safety concerns;<sup>7</sup> the National Highway Traffic Safety Administration routinely publicizes the names of companies responsible for airplane crashes. There are numerous other examples of appropriate disclosure.<sup>8</sup> It is high irony that public disclosure has made food consumption and airline travel extremely safe for Americans while a far greater danger, the threat of long-term blackout for millions, has been neglected by the responsible federal regulator, FERC.

Presently, NERC, as the designated ERO, is improperly using the Critical Energy/Electric Infrastructure Information (CEII) rule<sup>9</sup> to hide from public view the identities of entities that violate Critical Infrastructure Protection (“CIP”) Reliability Standards – even when the violation has been abated and there is no longer a security need to withhold this information. Essentially, NERC and the Regional Entities are misusing FERC’s authority to shield industry from public scrutiny. The Commission must not allow this practice repugnant to the public interest to continue.

### **Duke Energy Example – FERC Docket NP19-4-000**

On January 25, 2019, NERC filed a 250 page Notice of Penalty with FERC that disclosed 127 cybersecurity standard violations by an “unidentified registered entity.” NERC and its Regional Entities (RE) determined:

---

<sup>6</sup> U.S. Securities and Exchange Commission. <https://www.sec.gov/news/pressreleases> (accessed November 22, 2018).

<sup>7</sup> U.S. Food and Drug Administration. <https://www.foodsafety.gov/recalls/recent/index.html> (accessed November 22, 2018).

<sup>8</sup> U.S. National Highway Traffic Safety Administration. <https://www.nhtsa.gov/press-releases> (accessed November 22, 2018).

<sup>9</sup> 18 CFR § 388.113, et seq.

[T]he 127 violations collectively posed a serious risk to the security and reliability of the BPS (Bulk Power System). The Companies' violations of the CIP Reliability Standards posed a higher risk to the reliability of the BPS because many of the violations involved long durations, multiple instances of noncompliance, and repeated failures to implement physical and cyber security protections.

The NERC-imposed fine was \$10 million, tiny in comparison to Duke's 2017 net income of \$3 billion. It is notable that the Notice of Penalty revealed violations that could allow adversaries in remote locations to gain electronic access to grid facilities:

The REs determined that the Companies allowed interactive remote access to the BCSs (Bulk Electric System Cyber Systems) inside the Companies ESP (Electronic Security Perimeter) without first going through an Intermediate System, utilizing encryption, and requiring multi-factor authentication.

The violation started when the Standard became mandatory and enforceable and is *currently ongoing*. [Emphasis added.]

The violated standard, CIP-005-5-2 R2, became effective in July 2015. Without fear of public scrutiny, it is apparent that even three and one-half years have not been sufficient time for the "unidentified registered entity" to remedy this *currently ongoing* violation.

On February 1, 2019, trade publication *EnergyWire* disclosed that Duke Energy is the unnamed standards violator.<sup>10</sup> Duke Energy is one of America's largest utilities, with 7.2 million customers across seven states. Duke's generation fleet includes six nuclear plants. A physical or cyber attack on Duke could cause a long-term, wide-area blackout and result in release of radioactive contaminants. Nonetheless, the NERC standard enforcement regime, with its practice of hiding the names of violators under the guise of CEII, has failed to assure the protection of Americans depending on Duke for their electric power.

---

<sup>10</sup> Sobczak, Blake and Behr, Peter. "Duke agreed to pay record fine for lax security — sources" E&E News, February 1, 2019. <https://www.eenews.net/energywire/2019/02/01/stories/1060119265?fbclid> (accessed February 5, 2019).

## Pacific Gas and Electric Example – FERC Docket NP18-7-000

Another example of NERC abuse of the CEII rule is contained in FERC Docket NP18-7, which is hereby attached as Exhibits A-G. Also instructive are the events both before and after the docket. Let's start with the end of the story – the American public is informed.

On August 24, 2018, the *Wall Street Journal* ran a story titled: "PG&E Identified as Utility That Lost Control of Confidential Information." Subtitle: "As a result of 2016 failure, 30,000 records about PG&E's cyber assets were exposed on the internet."<sup>11</sup> This story stems from FERC Docket NP18-7, however, it required Herculean effort by citizens to force the disclosure of PG&E's identity. This should not have been the case.

Events leading to FERC Docket NP18-7 began on May 30, 2016 when cybersecurity expert Chris Vickery reported a massive data breach by Pacific Gas and Electric (PG&E).<sup>12</sup> According to Mr. Vickery:

Among other things, it contained details for over 47,000 PG&E computers, virtual machines, servers, and other devices. All of it completely unprotected. No username or password required for viewing. We're talking about IP addresses, operating systems, hostnames, locations, MAC addresses, and more. This would be a treasure trove for any hostile nation-state hacking group. That's not to mention the 120 hashed employee passwords, or the plaintext NTLM, SOAP, and mail passwords.

Any anonymous internet user—including those in North Korea, Iran or Russia—having free access to sensitive PG&E data is a grave national security violation. A cyber-attack on PG&E could cause a cascading collapse, resulting in a blackout for San Francisco, Silicon Valley, and much of the Western Interconnection.

On February 28, 2018 NERC issued a "Notice of Penalty regarding Unidentified Registered Entity"<sup>13</sup> in which the NERC-anonymized entity apparently agreed to pay penalties of \$2.7

---

<sup>11</sup> Smith, Rebecca. "PG&E Identified as Utility That Lost Control of Confidential Information." The Wall Street Journal. August 24, 2018. <https://www.wsj.com/articles/pg-e-identified-as-utility-that-lost-control-of-confidential-information-1535145850> (accessed November 22, 2018).

<sup>12</sup> Vickery, Chris. "Pacific Gas and Electric Database Exposed." <https://mackeeper.com/blog/post/231-pacific-gas-and-electric-database-exposed> (accessed November 28, 2018).

<sup>13</sup> Attached as Exhibit A.

million for very serious cybersecurity violations. According to NERC, this data breach 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 [Unidentified Regulated Entity’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.

By the time of NERC’s submission of its February 28, 2018 “Notice of Penalty regarding Unidentified Registered Entity,” the breach had been mitigated and there was no longer an access vulnerability.<sup>14</sup> According to a federal regulation, 18 CFR § 39.7 (b)(4), at the point where “Notice of Penalty regarding Unidentified Registered Entity” was submitted to FERC, the identity of the “URE” should have been disclosed.

NERC cannot argue that its February 28, 2018 “Notice of Penalty regarding Unidentified Registered Entity” should be a non-public proceeding related to a “cybersecurity incident”<sup>15</sup> as it does not meet the regulatory definition of a “cybersecurity incident.”<sup>16</sup> According to NERC, this incident was a not “malicious act” as the definition of “cybersecurity incident” requires –

---

<sup>14</sup> *Id.* At 4-5.

<sup>15</sup> 18 CFR § 39.7(e)(7)

<sup>16</sup> 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.”

rather it was a colossal blunder on the part of the regulated entity. The public had the right to know who endangered them.

Despite the interventions and protests of several citizens and groups in Docket NP18-7<sup>17</sup>, the matter was closed without review by the Commission on May 30, 2018<sup>18</sup> and the name of the “Unidentified Registered Entity” was never disclosed on NERC’s website or in FERC’s public docket.

Below is the information as it appears on NERC’s public website about FERC Docket NP18-7:<sup>19</sup>

Date	Regulatory Authority	Regulatory Filing ID	Region	Registered Entity	NCR ID	Total Penalty (\$)	NERC Violation ID	Reliability Standard
2/28/2018	FERC	NP18-7-000 <a href="#">View Filing</a> >> <a href="#">View Notice</a> >>	WECC	Unidentified Registered Entity	NCRXXXXX	\$2,700,000	WECC2016016233	CIP-003-3
							WECC2016016234	CIP-003-3

It took a Freedom of Information Act (FOIA) request by this petitioner, and an appeal of the denied request, to conclusively determine the identity of the standards violator: PG&E, one of America’s largest utilities.

## Numerous Other Examples of Secret Enforcement Actions

In fact, analysis of NERC enforcement actions between 2010 and 2018 reveals a multitude of cases in which NERC hid the identities of the “registered entities” that violated reliability standards.<sup>20</sup> Many of these enforcement actions involved settlements for substantial penalties, yet the settlement agreements were not disclosed either.

<sup>17</sup> Attached as Exhibits C-F.

<sup>18</sup> 163 FERC ¶ 61,153, attached as Exhibit G.

<sup>19</sup> [https://www.nerc.com/pa/comp/CE/Pages/Actions\\_2018/Enforcement-Actions-2018.aspx](https://www.nerc.com/pa/comp/CE/Pages/Actions_2018/Enforcement-Actions-2018.aspx) (accessed December 9, 2018)

<sup>20</sup> 2014: [https://www.nerc.com/pa/comp/CE/Pages/Actions\\_2014/Enforcement-Actions-2014.aspx](https://www.nerc.com/pa/comp/CE/Pages/Actions_2014/Enforcement-Actions-2014.aspx);

2015: [https://www.nerc.com/pa/comp/CE/Pages/Actions\\_2015/Enforcement-Actions-2015.aspx](https://www.nerc.com/pa/comp/CE/Pages/Actions_2015/Enforcement-Actions-2015.aspx);

2016: [https://www.nerc.com/pa/comp/CE/Pages/Actions\\_2016/Enforcement-Actions-2016.aspx](https://www.nerc.com/pa/comp/CE/Pages/Actions_2016/Enforcement-Actions-2016.aspx);

2017: [https://www.nerc.com/pa/comp/CE/Pages/Actions\\_2017/Enforcement-Actions-2017.aspx](https://www.nerc.com/pa/comp/CE/Pages/Actions_2017/Enforcement-Actions-2017.aspx);

2018: [https://www.nerc.com/pa/comp/CE/Pages/Actions\\_2018/Enforcement-Actions-2018.aspx](https://www.nerc.com/pa/comp/CE/Pages/Actions_2018/Enforcement-Actions-2018.aspx) (accessed December 9, 2018).

Exhibit O Lists 243 FERC dockets and at least 1,465 “Unidentified Registered Entities” related to these dockets who violated CIP standards between 2010 and 2018. None of these “Unidentified Registered Entities” has yet been identified to the public by either NERC or FERC even though they have been subject to regulatory action overseen by the United States government. These actions all claim that the violations have been “mitigated,” so there is absolutely no national security argument that the identities of these entities and the settlement agreements should still be withheld from the public.

Moreover, NERC cannot argue – as they are attempting to argue in the January 25, 2019 Duke Energy NOP (Docket Number NP19-4-000) – that these should be non-public proceedings related to “cybersecurity incidents.”<sup>21</sup> None of these 243 regulatory actions involve “cybersecurity incidents” as defined in the regulation. These dockets were regulatory actions resulting from audits or self-reports – not “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” as defined at 18 CFR § 39.1. NERC is simply misapplying this FERC regulation in an attempt to shield the industry from proper public scrutiny.

A review of the publicly available information on these dockets reveals troubling issues; however, without the disclosure of the names of the entities and the text of settlement agreements, it is impossible for the public to fully appreciate how standards violations by utilities place lives at risk. Here are some examples:

- Since the Metcalf substation attack on PG&E on April 16, 2013, one would think that there would be utility focus on physical security for high voltage transformers – most of which are guarded only by a chain link fence and crossed fingers. So exactly how many enforcement actions would you guess there have been in the last 5 years for “CIP-014” physical security? Only one. (FERC Docket NP18-14-000.)

---

21



- Many of the “penalties” result from settlement agreements (e.g., the “Unidentified Registered Entity” agrees to pay the “penalty” and in many cases does not admit fault for the violation). Without knowing the details of the settlement agreements, the public cannot adequately analyze the terms and penalties, or even identify offending utilities.
- In some of the cases that were “settled,” the regulated entities were “uncooperative” (FERC Docket NP16-12-000) or “not fully transparent and forthcoming” (FERC Docket NP18-7-000). “Settling” with such bad actors raises many regulatory red flags and the public needs to analyze these FERC-approved transactions in more detail.
- I have found numerous examples of *non-CIP violations* that have been redacted. For example, I have found at least four violations of vegetation management standards for transmission lines in the Western Interconnection<sup>22</sup> – the same region where over 86 deaths occurred in the “Camp Fire” – the deadliest and most destructive wildfire in California history. This is the same region where a “regulated entity” (PG&E) has significant liability for wildfires. The public has a right to know who standard violators are, especially when the standards violations may have resulted in dozens of deaths.

After this NERC cover up started in July of 2010, there has been *less incentive to fix the grid security problems*. That’s why disclosure is important. Why should utilities spend money to fix grave cybersecurity issues if they know that 1) if caught, the friendly regulator will “settle” the violation privately and the settlement agreement will be kept secret, 2) the utility can negotiate a trivial fine, and 3) the utility’s name will not be disclosed to the public?

## **Federal Regulations Require Disclosure**

18 CFR § 39.7 (b)(4) provides 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.]

---

<sup>22</sup> See FERC Docket Numbers: NP11-1-000; NP11-128-000; NP11-137-000 and NP12-20-000.

Further, 18 CFR § 39.7(d)(1) provides that a notice of penalty by the Electric Reliability Organization shall consist of, *inter alia*: “The name of the entity on whom the penalty is imposed.”

The federal regulations are very clear that the name of the entity on whom the NERC penalty is imposed must be disclosed. Yet, somehow NERC has apparently been excused from complying from federal regulations. How has this happened?

Even the Commission’s own interpretation of the Critical Energy Infrastructure Information (CEII) rules support disclosure. 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).<sup>23</sup>

Nevertheless, in July 2010 FERC began allowing NERC to hide the identity of the “Unidentified Registered Entities.” Further, as described below, *NERC claims FERC instructed this change in policy.*

NERC’s concealments are against the public interest and should never have been allowed by FERC. The PG&E data breach in 2016 and NERC’s cover-up of the identity of the “Unidentified Registered Entity” in FERC Docket NP18-7-000 — a standard violation by NERC’s own admission that endangered the bulk power system — is clearly against the public interest. Likewise for the coverup of 127 cybersecurity violations of Duke Energy exposed by the press in January 2019. The public must be able to cast scrutiny over the activities of NERC and its regulated entities for the self-regulatory scheme codified in Section 215 to be effective.

## **Disclosure of Violators’ Identity Should Be the Default Practice**

In the PG&E example, disclosure of the identity of the “URE” took a Freedom of Information Act (FOIA) request and a subsequent appeal by the petitioner. Attached as exhibits are the initial

---

<sup>23</sup> FERC Order No. 833 at pg. 17. Also see 18 C.F.R. §388.113(c)(1)(iv).

request (Exhibit H), FERC's April 23, 2018 submitter rights letter to NERC (Exhibit I), NERC's April 30, 2018 Response Letter to FERC (Exhibit J), FERC's May 25, 2018 response letter to me denying the FOIA request in its entirety (Exhibit K), my June 16, 2018 appeal of FERC's determination (Exhibit L), FERC's August 2, 2018 response letter granting my appeal in part – specifically agreeing to disclose the identity of the URE (Exhibit M), and the August 24, 2018 FERC disclosure of the requested information (Exhibit N).

Notably, FERC's initial denial of the FOIA request on May 25, 2018 was based on NERC's very puzzling interpretation of FERC's policy. I am including NERC's objection below in its entirety:

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). [Emphasis added.]

The statement that “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” is completely unsupported by any reasonable read of 149 FERC ¶61,141. This order simply does not state or imply in any way that the Commission has ever given NERC any such instruction. And, to the extent that the NERC Rules of Procedure conflict with 18 CFR § 39.7, the federal regulation must take precedence. A corporation's “procedures” do not trump federal regulations.<sup>24</sup>

---

<sup>24</sup> Perhaps FERC or one of its Commissioners gave an “off-the-record” instruction to NERC to conceal the identity of standards violators. If NERC continues to claim an exemption from 18 CFR § 39.7 in future filings, this is a matter that should be investigated by the Department of Energy's Office of the Inspector General.

While this slight of pen on the part of NERC's attorneys may have misled the Commission's staff into denying the initial FOIA request on May 25, 2018 (Exhibit D), on appeal, the Commission's general counsel correctly concluded "that the name of the URE can be disclosed" on August 2, 2018 (Exhibit F).

However, this one FOIA disclosure in this one instance is not enough to abate NERC's abhorrent practice of routinely concealing information from the public – which continues to this day. FERC regulations, while seemingly clear, have been abused by NERC and the Regional Entities to the point of creating a "new normal." Clarification by means of a formal rulemaking is needed.

### **FERC's Mandate to Act in the Public Interest**

16 U.S.C. § 824o(d)(2) provides that: "The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest." [Emphasis added.]

Thus, FERC is charged with serving the public interest. Not the interests of NERC and/or the electric utility industry. The public interest demands that information on industry practices, successes, failings and regulatory actions be available for public scrutiny. This is especially the case in the electric utility industry on which every American is dependent – and indeed, pays for.

In order to serve the public interest, the Commission should not allow NERC and the electric utility industry to continue to hide the identities of regulated entities that are subject to regulatory actions.

### **Conclusion**

I request that the Commission issue a declaratory order or rule clarifying that the names of regulated entities subject to regulatory actions by the Commission or by the Electric Reliability Organization ("ERO") shall be publicly disclosed, along with the full text of settlement

agreements. Continuing assessments by the U.S. intelligence community make it clear that our electric grid is not secure. By allowing NERC to hide the identities of utilities that violate grid security standards, FERC is failing in its duty to the American public. Free of public scrutiny, utilities do not correct security shortfalls for months and even years; the regulatory system is broken. Now is the time to end NERC's apparently illegal scheme that hides the names of the violators of grid security standards.

Respectfully submitted by:



Michael Mabee

Exhibits:

- A. February 28, 2018 NERC Full Notice of Penalty regarding Unidentified Registered Entity
- B. March 30, 2018 FERC Notice (162 FERC ¶ 61,291)
- C. April 15, 2018 Motion to Intervene of Michael Mabee
- D. April 15, 2018 Motion to Intervene and Comment of Public Citizen, Inc. and The Utility Reform Network
- E. May 29, 2018 Comments of Isologic, LLC and the Foundation for Resilient Societies
- F. May 29, 2018 Comments of Frank J. Gaffney
- G. May 30, 2018 FERC Notice (163 FERC ¶ 61,153)
- H. April 13, 2018 FOIA Request (FOIA No. FY18-75)
- I. April 23, 2018 FERC Submitter Rights Letter to NERC
- J. April 30, 2018 NERC Response Letter to FERC
- K. May 25, 2018 FOIA Response Letter
- L. June 16, 2018 Appeal of Determination in FOIA No. FY18-75
- M. August 2, 2018 FERC Response Letter
- N. August 24, 2018 FERC Response Letter
- O. 246 FERC Dockets involving "Unidentified Registered Entities" 2010-2018

**Exhibit A**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

February 28, 2018

**VIA ELECTRONIC FILING**

Ms. Kimberly D. Bose  
Secretary  
Federal Energy Regulatory Commission  
888 First Street, N.E.  
Washington, DC 20426

**Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity,  
FERC Docket No. NP18-\_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty<sup>1</sup> regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).<sup>2</sup>

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,<sup>3</sup> with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of two violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards.

---

<sup>1</sup> *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). See also 18 C.F.R. Part 39 (2017). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). See 18 C.F.R § 39.7(c)(2).

<sup>2</sup> See 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

<sup>3</sup> For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

3353 Peachtree Road NE  
Suite 600, North Tower  
Atlanta, GA 30326  
404-446-2560 | [www.nerc.com](http://www.nerc.com)

NERC Notice of Penalty  
 Unidentified Registered Entity  
 February 28, 2018  
 Page 2

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
 HAS BEEN REMOVED FROM THIS PUBLIC VERSION

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two million seven hundred thousand dollars (\$2,700,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

### Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

Violation(s) Determined and Discovery Method						
*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation						
NERC Violation ID	Standard	Req.	VRF/VSL	Discovery Method*	Risk	Penalty Amount
WECC2016016233	CIP-003-3	R4	Medium/ Severe	SR	Serious	\$2.7M
WECC2016016234	CIP-003-3	R5	Lower/ Severe			

### Background to the Violations

URE received a report of an online data exposure with data possibly associated with URE. The report came from a white hat security researcher not associated with URE. A third-party URE contractor exceeded its authorized access by improperly copying certain URE data from URE's network environment to the contractor's network environment, where it was no longer subject to URE's visibility or controls. The contractor failed to comply with URE's information protection program on which it was trained. While the data was on the contractor's network, a subset of live URE data was accessible online without the need to enter a user ID or password. This subset of data included over



NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 3

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

30,000 asset records, including records associated with Critical Cyber Assets (CCAs). The records included information such as IP addresses and server host names.

The information associated with the CCAs was accessible on the Internet for a total of 70 days. URE also reviewed the system logs of the contractor and found that the logs showed unauthorized access to the URE data subset from unknown IP addresses, as well as IP addresses associated with the white hat security researcher who notified URE of the data exposure.

URE informally notified WECC of the incident and explained how URE was managing the situation. URE and WECC had multiple discussions and meetings about the situation over the next two months. Four months after it had discovered the incident, URE submitted an incident update to WECC.

Based on information from URE's incident report and WECC data requests, WECC recommended URE file Self-Reports for the issues. WECC determined URE failed to implement adequately its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-3 R4. WECC also determined URE failed to implement adequately a program for managing access to protected information related to CCAs, as required by CIP-003-3 R5.

Analysis of the system logs showed that only the security researcher executed commands to view and download data. More detailed system logs would be required to determine definitively that no other third party had downloaded the data, but the short duration of the connections decreased the likelihood that additional accessing or downloading of data had occurred. To recover the exposed data, URE contacted the security researcher and requested that he securely return the data, securely delete all copies of the data from his system, and submit to URE a signed, notarized affidavit confirming that he deleted all copies of the data.

#### RISK COMMON TO THE VIOLATIONS

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

NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 4

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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.

WECC found URE had implemented limited compensating controls to reduce the risk associated with a malicious actor gaining access to its system during the noncompliance. URE did not classify the data as CIP-protected information because it was on a pre-production server, nor were there any controls in place to prevent the contractor from taking the data off premises and putting it on their own Internet-facing network. URE had implemented simple-character usernames similar to the usernames that were publicly exposed. In addition, URE did not implement any preventive or detective controls. URE only discovered the data exposure because of an external white hat security researcher who found the publicly accessible data on the Internet.

URE has three firewalls between the external network and the assets inside the Electronic Security Perimeter that make it difficult for a malicious actor to access URE's CCAs. Based on the controls WECC analyzed, there was lower probability that this instance of noncompliance would have caused an impact to the reliability of the BPS at the time of its occurrence. Nevertheless, there is no reasonable assurance that during the time the data was exposed on the Internet, it was not already used by a malicious actor – or collected by such an actor – to access URE's network and install an application that can cause the potential harm in the future. The additional sanction described below is intended to address this residual risk.

#### MITIGATION ACTIVITY COMMON TO THE VIOLATIONS

URE submitted identical Mitigation Plans to address the referenced violations. To mitigate these violations, URE:

1. Required the vendor to shut down their software development server, thereby ending the data exposure;
2. Performed three different forensic analyses to verify that only the security researcher accessed the data during the time of the exposure;
3. Required the security researcher to provide the data to the IT department, delete the data from his computer, and attest in an affidavit that these items were complete;
4. Removed vendor access to the asset management database in the datacenter. To allow vendors to perform development work on projects, URE implemented a process whereby an authorized URE employee must copy the source code from the asset management database and securely transfer it to the software development vendor. Upon work

NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 5

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

completion, the vendor would then securely transfer the new version of code to an authorized URE employee who would load it back onto the asset management database;

5. Changed access controls to the database. URE also deployed a suite program to provide policies and controls to prevent confidential-Bulk Electric System (BES) Cyber System Information or restricted-BES Cyber System Information classified emails and attachments from being sent to outside email addresses;
6. Improved security controls for vendor management by requiring vendors to take information security and privacy awareness training annually, implementing a new vendor remote access platform, and enhancing policies, background checks, and contract language for vendor employees; and
7. Classified all BES Cyber System Information for both production and non-production assets.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

#### VIOLATION DESCRIPTIONS

##### CIP-003-3 R4 - OVERVIEW

WECC determined that URE did not adequately implement its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-3 R4. Specifically, in the above described incident, WECC found that URE failed to adequately implement the following areas of its program to identify, classify, and protect information associated with CCAs:

1. URE failed to identify and classify the information used in the system in accordance with its information protection policy. URE stated it did not classify in accordance with its policy because the information was part of a pre-production asset management system. Even though the data was in a pre-production system, it is live CCA Information, and URE was required to implement a program to identify, classify, and protect this information.
2. Due to URE's failure to classify the information, URE also failed to provide the proper protections during storage and transmission, distribution, and duplication, in accordance with its policy.
3. URE failed to designate the system and the contractor's network IP as a CCA Information approved storage location and store CCA Information in an approved location.
4. URE failed to ensure that personnel handling CCA Information adhered to URE's protection measures.

NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 6

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

5. URE failed to activate its existing policies or procedures for sharing protected information with third parties before information was disseminated, either electronically or physically, in accordance with its policy.

The cause of this violation was URE's failure to apply its information protection program to the CCA Information in its pre-production environment.

WECC determined that this violation posed a serious and substantial risk to the reliability of the BPS.

WECC determined the duration of the violation to be approximately 590 days, from the date the third-party contractor exposed the information on the Internet, through when URE completed classifying all CCA Information for production and non-production assets. WECC cannot confirm that another third party did not capture and retain possession of the exposed data.

#### CIP-003-3 R5 - OVERVIEW

WECC determined that URE did not implement a program for managing access to protected CCA Information, as required by CIP-003-3 R5. Specifically, in the above described incident, WECC found that URE failed to ensure that the contractor protected the CCA Information when it improperly copied the data from URE's network environment to the contractor's network environment, where it was no longer subject to URE's visibility or controls. In response to a data request, due to the fact that the contractor copied the data to an unapproved location, URE stated that the security controls for the contractor's storage location were not understood or documented. WECC found that URE did not understand or document the security controls at the contractor's location before it released information to the contractor, and afterward, when the data was exposed to the Internet, it failed to adequately implement its program for managing access.

The cause of this violation was URE's failure to ensure its contractor followed its information protection program and procedures on which the contractor was trained.

WECC determined that this violation posed a serious and substantial risk to the reliability of the BPS.

WECC determined the duration of the violation to be approximately 80 days, from the date the third-party contractor exposed the information on the Internet, through when the white hat security researcher deleted all remaining electronic copies of data and screen shots from his hard drive and sanitized his device to prevent future access. WECC cannot confirm that another third party did not capture and retain possession of the exposed data.

NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 7

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

### Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two million seven hundred thousand dollars (\$2,700,000) for the referenced violations as well as a non-monetary sanction. As an additional sanction designed to reduce the opportunities for a malicious actor to use the exposed data, WECC required URE to set its relevant CIP passwords-remembered to "all" or the maximum the system will remember to prevent passwords from being used more than once, or to maximize the frequency for which a password may be used.

In reaching this determination, WECC considered the following factors:

1. the instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE had an internal compliance program at the time of the violation;
3. URE self-reported the violations;
4. URE was not fully transparent and forthcoming with all pertinent information detailing the data exposed in the incident. Specifically, URE did not provide WECC initially with all the data fields exposed in the incident;
5. the violations posed a serious and substantial risk to the reliability of the BPS; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two million seven hundred thousand dollars (\$2,700,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 8

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

## Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed<sup>4</sup>

### Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,<sup>5</sup> the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on February 6, 2018, and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two million seven hundred thousand dollars (\$2,700,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

---

<sup>4</sup> See 18 C.F.R. § 39.7(d)(4).

<sup>5</sup> *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 9

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

**Notices and Communications:** Notices and communications with respect to this filing may be addressed to the following:

<p>Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz</p> <p>Steve Goodwill* Vice President and General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6857 (801) 883-6894 – facsimile sgoodwill@wecc.biz</p> <p>Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile raredondo@wecc.biz</p> <p>Heather Laws* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz</p>	<p>Sonia C. Mendonça* Vice President, Acting General Counsel and Corporate Secretary, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net</p> <p>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 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net</p> <p>Leigh Anne Faugust* Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@nerc.net</p>
--	--

NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 10

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

\*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.



NERC Notice of Penalty  
Unidentified Registered Entity  
February 28, 2018  
Page 11

NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

### Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Leigh Anne Faugust

Sonia C. Mendonça  
Vice President, Acting General Counsel and  
Corporate Secretary, and Director of  
Enforcement  
Edwin G. Kichline  
Senior Counsel and Director of  
Enforcement Oversight  
Leigh Anne Faugust  
Counsel  
North American Electric Reliability  
Corporation  
1325 G Street N.W.  
Suite 600  
Washington, DC 20005  
(202) 400-3000  
(202) 644-8099 - facsimile  
sonia.mendonca@nerc.net  
edwin.kichline@nerc.net  
leigh.faugust@nerc.net

cc: Unidentified Registered Entity  
Western Electricity Coordinating Council

Document Content(s)

Public\_CIP\_NOC-2569 Full NOP.PDF.....1-11

**Exhibit B**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

162 FERC ¶ 61,291  
UNITED STATES OF AMERICA  
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation

Docket Nos. NP18-7-000  
NP18-8-000

NOTICE

(March 30, 2018)

Take notice that the Commission will not further review, on its own motion, the following Notice of Penalty:

<u>Docket No.</u>	<u>Filing Date</u>	<u>Registered Entity</u>
NP18-8-000	February 28, 2018	Spreadsheet NOP

However, pursuant to 18 C.F.R. § 39.7(e)(1) (2012), the Commission is extending 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.

If no further action is taken by the Commission in this matter by that date, the penalty will be deemed affirmed by operation of law.

By direction of the Commission.

Nathaniel J. Davis, Sr.,  
Deputy Secretary.

Document Content(s)

NP18-7-000.DOCX.....1-1

**Exhibit C**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

<b>NERC Full Notice of Penalty regarding</b>	)	
<b>Unidentified Registered Entity</b>	)	<b>Docket No. NP18-7-000</b>
	)	

**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)<sup>1</sup>. 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.<sup>2</sup> 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”<sup>3</sup> 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 breach 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 Publicly Available Information Which Should Trigger Commission Review

1. Prompt reporting requirement: It is unclear from the publicly 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).<sup>4</sup> We also note that the name of the entity has been widely speculated in the media.<sup>5</sup> 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"<sup>6</sup> as this does not meet the regulatory definition of a "cybersecurity incident."<sup>7</sup> 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

---

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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](http://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_NOC-2569%20Full%20NOP.pdf) (accessed April 7, 2018).

<sup>4</sup> Order No. 833 at pg. 17. Also see 18 C.F.R. §388.113(c)(1)(iv).

<sup>5</sup> 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).

<sup>6</sup> 18 CFR § 39.7(e)(7)

<sup>7</sup> 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)

FERC Docket NP18-7 (Final).PDF.....1-3

**Exhibit D**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation

Docket No. NP18-7

**Motion to Intervene and Comment of Public Citizen, Inc. and The Utility Reform Network (TURN)**

On March 30, 2018, the Commission issued a Notice that it was extending the time period for consideration whether to review the Notice of Penalty that NERC filed with the Commission on February 28, 2018 in Docket No. NP18-7.

Public Citizen, Inc. and The Utility Reform Network (TURN) submit this Motion to Intervene and Comment. We request that the Commission require public disclosure of the names of the utility and contractor at the center of the Notice of Penalty in this Docket, as publicly revealing the names of the offenders is necessary for the benefit of the public interest.

**Motion to Intervene**

Public Citizen is a not-for-profit, public interest research and advocacy organization representing the interests of our more than 400,000 members and supporters across the United States. Public Citizen frequently intervenes and comments in FERC dockets.

TURN is a not-for-profit, public interest advocacy organization representing the interests of residential customers of investor-owned gas, electric, telecommunications and water utilities serving end-use customers in California. For the past 40 years, TURN has intervened in proceedings at the California Public Utilities Commission on behalf of residential customers in a wide array of proceedings relating to utility cost recovery and ratemaking. TURN has approximately 20,000 individual members and regularly appears before state agencies, the Legislature, and the California Independent System Operator.

**Background**

The Notice of Penalty NERC filed with the Commission stems from a Settlement Agreement between the Western Electricity Coordinating Council (WECC) and an Unidentified Registered Entity (URE) regarding “serious and substantial” violations of the Critical

Infrastructure Protection NERC Reliability Standards [NERC Notice of Penalty, at Page 6]. The violations involve a third-party contractor hired by the URE, and the identity of this contractor is also kept secret in the NERC Notice of Penalty. These violations prompted a settlement agreement where the URE agreed to pay a \$2.7 million penalty. According to a media report, this penalty is described as “massive” and unprecedented, and represents by far the largest penalty ever assessed for a CIP reliability standard violation.<sup>1</sup>

The only reason the WECC, NERC, the URE and the URE’s contractor even knew about the breach was because of the actions of an unrelated “white hat” hacker that uncovered the contravention and notified the URE. The URE only saw fit to initially “informally” notify the WECC of the white hat’s discovery, and then waited four months to finally file a formal report to the WECC [NERC Notice, at Page 3].

The URE’s cybersecurity violations created vulnerabilities that could have allowed hackers to gain “both physical and remote access” to its systems [NERC Notice, at Page 3]. In all, more than 30,000 records were left exposed on the public internet for 70 days, including Critical Cyber Assets [NERC Notice, at Page 3].

### **The Need for Public Disclosure of the Names of the Offenders**

18 C.F.R. § 39.7(b)(4) states: “Each violation or alleged violation shall be treated as nonpublic until the matter is filed with the Commission as a notice of penalty . . . The disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk-Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise” [emphasis added]. Public Citizen and TURN ask that the Commission direct the public release of the name of the URE and its contractor under 18 C.F.R. § 39.7(b)(4) for the reasons outlined below.

First, if the URE is an electric utility subject to state rate regulation, keeping its name secret may mean that the state regulatory commission with jurisdiction over the URE does not know about the violation and the assessed penalty. Keeping the identity of the URE non-public from state utility regulators and from customer intervenors participating in state utility commission proceedings could allow the URE to seek retail rate recovery for such costs. Absent

---

<sup>1</sup> Blake Sobczak and Sam Mintz, “Grid regulator issues 'massive' penalty over data exposure,” *E&E News*, March 5, 2018.

the knowledge of the violation, the state utility commission would be unable to assess whether these costs are properly recovered from ratepayers or should be borne by shareholders. This outcome would defeat the entire purpose of the Penalty by forcing ratepayers to absorb the costs of utility imprudence. Furthermore, to the extent that the URE submits cybersecurity-related rate recovery requests to state utility regulators, knowing a URE's track record on such issues may materially affect regulators' assessment of such requests.

Second, if media reports are accurate that the penalty is the largest ever on record for a cybersecurity-related offense, then it is in the public interest to reveal the identity of the violator. Concealing the name of the recipient of the largest fine in history sends a confusing message to the public that large penalties do not come with full accountability, as future violators may be able to similarly hide behind of the veil of anonymity.

Third, directing the public release of the name of the URE will not jeopardize cybersecurity, the security of the Bulk-Power System, or national security. The violations described in the NERC Notice of Penalty do not identify any current or recurring vulnerabilities; rather, they stem from the one-time actions of a URE contractor that improperly handled cybersecurity data. In fact, public release of the name of the URE could *improve* cybersecurity, as regulators and stakeholders could use such public information to better educate and prepare the URE and other utilities' practices. In general, the more information that regulators and the public have about violators, the better able we all are to learn from past mistakes and reduce the likelihood of future ones. But keeping state regulators and the public in the dark about the cybersecurity track record of our electric utilities may actually create a false sense of security, and reduce the likelihood of more public awareness and vigilance needed to protect cybersecurity.

Fourth, for similar reasons, the identity of the URE contractor should also be made public. Although the NERC Notice of Penalty does not apparently involve penalties for the unnamed contractor, the Notice details a significant role that the contractor played in causing the violations. Keeping the identity of the contractor non-public shields the company from any additional scrutiny of its track record from state regulators, consumer advocates and members of the public, particularly if the vendor has other, existing relationships with other utilities. Directing the public release of the name of the contractor will better equip state regulators and

the general public to help ensure the contractor maintains the highest standards for caretaking cybersecurity operations and data.

Fifth, public media reports appear to identify the name of the URE. A June 1, 2016 blog identifies PG&E as an electric utility that suffered an inadvertent exposure of cybersecurity data in circumstances that appear very similar to the one described in the NERC Notice of Penalty<sup>2</sup>. A subsequent *E&E News* article interviews a “white hat” hacker who details violations by PG&E that are very similar to the ones described in the NERC Notice of Penalty.<sup>3</sup> If the identity of the URE has already been publicly identified, than Commission action to direct the public release of the name of the URE would be a mere formality, and help alleviate any confusion about similarities between the data breach that identifies PG&E and a similar violation described in the NERC Notice of Penalty.

Respectfully submitted,

Tyson Slocum, Energy Program Director  
Public Citizen, Inc.  
215 Pennsylvania Ave SE  
Washington, DC 20003  
(202) 588-1000  
tslocum@citizen.org

Matthew Freedman, Staff Attorney  
The Utility Reform Network  
785 Market St #1400  
San Francisco, CA 94103  
(415) 954-8084  
matthew@turn.org

---

<sup>2</sup> <https://mackeeper.com/blog/post/231-pacific-gas-and-electric-database-exposed>

<sup>3</sup> Blake Sobczak and Sam Mintz, “Grid regulator issues 'massive' penalty over data exposure,” *E&E News*, March 5, 2018.

Document Content(s)

NERCpenalty.DOCX.....1-4



**Exhibit E**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

<b>NERC Notice of Penalty regarding</b>	)	<b>Docket Nos. NP18-7-000, RM18-2-000,</b>
<b>Unidentified Registered Entity</b>	)	<b>AD17-9-000, RM17-13-000</b>

**Comments of Isologic, LLC and the Foundation for Resilient Societies, Inc. on a Notice of  
Penalty for an Unidentified Registered Entity**

(submitted to FERC on May 29, 2018)

The undersigned provide the following Comments, without a formal Motion to Intervene, because we recognize that the decision to name a presently “Unidentified Registered Entity” is discretionary among the Commissioners, and a decision to retain a *de minimus* penalty as proposed by a regional entity, the Western Electricity Coordinating Council (hereafter “WECC”), is also discretionary in the sole decision-making of the Commission.

So we do not seek to Intervene formally, but seek to persuade the Commissioners of the Federal Energy Regulatory Commission (hereafter “FERC” or “the Commission”) that they are at an important crossroad, signaling to the registered entities of the bulk power system, their vendor-contractors, the regional enforcement institutions, and the relevant state Public Utilities Commissions that FERC emphatically rejects a culture of insensitivity to inadequate cybersecurity and cyber-physical protections that can put entire grid Interconnections and the nation at risk. Or not.

Will FERC, with many new Commissioners now in office, determine whether to harness the power and accountability that flows from *transparency* by publicly naming both the “Unidentified Registered Entity” and their contractor-vendor which recklessly exposed an entire topology of grid network assets and communication links to potential cyber and cyber-physical attack? Or will FERC relapse into the presumption of anonymized fines that to the public signals and amplifies fears of *regulatory capture* by the *regulated* of the *regulators*? Does the

Commission now recognize the disinfecting role of public transparency as a foundational resource in fulfilling the Commission's mandate to maintain reliable operation of the bulk electric system (BES)?

## **Who We Are**

*Isologic* LLC is a limited liability company registered in the State of Maryland. It has a ten-year record of White Papers addressing *Security in the North American Grid*; physical, energy supply and most importantly cybersecurity. These White Papers have documented the evolution of Critical Infrastructure Standards (CIP) since the creation of the program by the Energy Policy Act of 2005. *Isologic* LLC has commented in filings with FERC on Notices of Proposed Rulemakings (NOPRs), Final Rules, and major related technical and policy issues involving cybersecurity issues and programs. Recent *Isologic* LLC filings on open dockets<sup>1</sup> include Incidence Reporting and Supply Chain standards which are relevant to this request to Intervene in the FERC Review of a penalty assessed in a significant security breach involving an Unidentified Responsible Entity (hereafter "URE") and its unidentified contractor-vendor who together caused the exposure of critical assets, network relationships, and communication links that apparently extended over more than 84 weeks or about 590 days.

The *Foundation for Resilient Societies, Inc.* (hereafter "Resilient Societies") is a research and education non-profit incorporated in New Hampshire in March 2012. Its primary mission is to develop understanding of vulnerabilities and remedies to strengthen the reliability and resilience of critical infrastructures, particularly in but not exclusively in the United States. In the month before the tsunami at Fukushima Dai-Ichi, Japan, we filed a draft Petition for Rulemaking with the Nuclear Regulatory Commission, finally accepted by that Commission in December 2012, to strengthen backup-power capabilities to mitigate and recover from solar geomagnetic storms. We have subsequently filed on improvements in physical security, cybersecurity, and other reliability standards, including criteria for cost recovery or resilient

---

<sup>1</sup> NOPR Cyber Security Incident Reporting Reliability Standards Docket Nos. RM18-2-000 and AD17-9-000 Issued December 21, 2017

capacity auctions to strengthen flexibility, adaptability, and recovery from threats to critical infrastructure operability. Further information is available at [www.resilientsocieties.org](http://www.resilientsocieties.org).

## Background

On February 28, 2018, the North American Electric Reliability Corporation (hereafter “NERC”) filed with FERC a Notice of Penalty<sup>2</sup>, with information and details regarding Western Electricity Coordinating Council (WECC) and the URE having entered into a Settlement Agreement **“to resolve all outstanding issues arising from WECC’s determination and findings of two violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards.”** The NERC filing asserted, without further comment, that the **“URE neither admits nor denies the violations, but has agreed to the assessed penalty of two million seven hundred thousand dollars (\$2,700,000), in addition to other remedies and actions.”**

Facts of this security incident included in the NERC Notice of Penalty (NP) filing can be summarized as follows:

As part of an asset development effort, a URE contractor was given access to the URE asset DataBase (hereafter “DB”), which was subsequently transferred from the URE’s server over a URE network to the Vendor’s network. A 30,000 asset subset of that transferred DB was put on a vendor server that was freely accessible to the Internet (no ID or password [PW] was required). (URE permissions for any or all of this are not stated; however, URE asserted that its contractor failed to comply with URE’s information protection program on which it was trained.)

In May 2016, the existence of this open DB was discovered by a security researcher who downloaded it to his infrastructure.

The exposed DB was publicly available in 2016 for 70 days on the vendor’s network and an additional 10 days before deletion on the security researcher’s system.

---

<sup>2</sup> NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP18-07-000 filed on February 28, 2018, 162 FERC ¶ 61,291.

Data exposure included Critical Cyber Assets including ID's, passwords and (unspecified) cryptographic information.

Upon URE notification to the Western Electricity Coordinating Council (WECC), (one of two reliability authorities in the Western Interconnection), discussions and research into the incident ensued for a period of four months involving the URE, presumably its vendor, and the WECC. According to NERC: ***"analysis of the system logs showed that only the security researcher executed commands to view and download data. More detailed system logs would be required to determine definitively that no other third party had downloaded the data, but the short duration of the connections decreased the likelihood that additional accessing or downloading of data had occurred."***<sup>3</sup> However, it could not be conclusively shown that there was no compromise of the URE's asset data during the period of exposure on the vendor's or security researcher's sites.

The URE was instructed by WECC to self-report the incident and an incident report was filed by the URE with the WECC.

In its assessment of the incident, the WECC estimated the period of violation at 590 days, from the first exposure to CCA data on the vendor's internet site to the point where the URE completed mitigation by properly classifying and protecting CCA data. WECC ultimately concluded that the URE had violated Security Management standards specified in CIP 003-3 Requirement R4 (***implement a program to identify, classify and protect information associated with CCA assets***) and Requirement R5 (***implement a program for controlling access to CCA information.***) The WECC concluded that the violation posed a severe risk to the Bulk Electric system ("BES") and assessed a penalty of \$2.7M plus an additional sanction.

---

<sup>3</sup> IBID

## Additional Background

The security researcher and several media outlets have confirmed that the URE is, in fact, the Pacific Gas and Electric Company, San Francisco, CA.<sup>4</sup> In response to a query to FERC on whether the URE would be publicly identified, a FERC spokesman said ***“If the commission determines to take further action on a NERC notice of penalty, it may result in a subsequent FERC order or settlement providing more detail. However, commission investigations are non-public, so if they do not result in an order/settlement the specific details would not be public.”***

PG&E issued the following statement<sup>5</sup> in response to several media inquiries:

***“With this incident, it is important to know that none of PG&E’s systems were directly breached in any way and no customer or employee data was involved. A PG&E vendor was hosting an online demonstration using PG&E asset management data to show the capabilities of a platform that they were developing for us. This data contained information on PG&E’s technology assets, such as computers and servers. This data was exposed online by the vendor and was discovered by a third-party researcher. That researcher contacted PG&E security and was unintentionally misinformed that the data was non-sensitive, mocked-up data. We based this feedback on an initial response from the vendor stating that the information in the database was demo or “fake” data. Following further review, we learned that the data was not fake, removed it, and contacted the researcher to correct our statement. We continue working with all of our vendors to have appropriate procedures in place at all times.”***

In his blog<sup>6</sup> issued about the same time, the security researcher identified as MacKeeper researcher Chris Vickery noted that he discovered a MongoDB server exposed to the Internet with no administrator account password. The exposed information, which could have been accessed by anyone without authentication, included IP addresses, hostnames, MAC addresses,

---

<sup>4</sup> See for example, “Pacific Gas and Electric Claims Recent Data Breach Only Exposed Fake Details” Softpedia News May 31, 2016 01:55 GMT By Catalin Cimpanu

<sup>5</sup> Database of California Electric Utility Exposed Online, [Security Week](#) By Eduard Kovacs, May 31, 2016

<sup>6</sup> Pacific Gas and Electric Database Exposed, MACKEEPER 30 / 05 / 2016 UPDATE (Jun 1st)

locations, operating system data, and over 100 employee passwords. While some of the passwords were hashed, the expert also found ones stored in clear text. He informed PG&E that the unprotected database could not be fake since it also included more than 688,000 unique log entries. Vickery noted that the database was taken down on May 26th after PG&E was notified. Before this happened, he made a copy to forward to the DHS. (It is not clear if the DB was ever forwarded to DHS.)

## **Reasons for This Filing and Comments**

Media reports exposed factual gaps in initial reports of this security violation by the security researcher, PG&E, the WECC, and NERC. PG&E was apparently told by its vendor that the data used in their development was fake and said so publicly, but this was contested immediately by the researcher, with substantial detail on the massive breach as shown above. PG&E later retracted that claim. The PG&E mention of a ‘demonstration’ of the vendor’s development product, not commented on by the researcher, suggests the vendor moved some or all the DB to a separate server for demonstrations of its product. There was no information on whether or not the vendor’s product demonstration contained CCA information, and if the data was further compromised. In truth, the scope of the breach is scanty and unclear and only available from the researcher.

Extensive sanitization by WECC or NERC cannot be justified; either organization should have at least supported the researcher’s factual findings and whether the exposure of asset data was “capped”. The information of value to an adversary, if not the full data set, was already exposed. Confirmation has the obvious value of documenting the severity of the breach for basic understanding by the public, other utilities, and of course, PG&E clients and stockholders.

And as noted in the introduction, we find direct relevancy to outstanding security issues that are central to proposed rulemaking involving inadequate Critical Infrastructure Protection (CIP) standards, Incident Reporting, plus expansive discussion of Supply Chain vulnerabilities –all of which are prominent in this PG&E security issue.

The VPN/Filter malware just revealed<sup>7</sup> by E & E News is but another wake-up call to the industry, the WECC, NERC and FERC. How many examples of the Russian Federation swath of Grid attack systems are needed before defense of the nation's electric system become high enough priority for breaches such as the PGE case to be taken seriously as National Security incidents? Is there anyone on this green earth who really understands what PGE gave up in this breach? Paired with VPN/Filter, what hope is there that the lights will stay on during a serious US-Russian dust-up?

Admittedly, PG&E was institutionally unable to anticipate the frailty of its vendor's cybersecurity reliability; nonetheless, the vagueness of CIP 003-3 security management requirements; the ambiguity on security of interconnectivity across the BES coupled to NERC determination to rely solely on individual site security perimeters for Grid protection, contributed significantly to this violation. And note the following FERC statement<sup>8</sup> limiting vendor liability: ***"In addition, the Commission stated that NERC's response to the Order No. 829 directive should respect the Commission's jurisdiction under FPA section 215 by only addressing the obligations of responsible entities and not by directly imposing any obligations on non-jurisdictional suppliers, vendors or other entities that provide products or services to responsible entities."*** Such a statement is distinctly unhelpful in any serious efforts to address Supply Chain vulnerabilities; the principal attack vector of this nation's adversaries. Frankly, NERC is an industry organization and protects utilities' interests; FERC's basic responsibilities are significantly broader. The settlement, therefore, deserves far more careful review than is evident in NP documentation.

## Identity of Principals

With the receipt of the NP, FERC is obliged to identify PG&E as the security violator; particularly since the settlement negotiated by the WECC and approved by NERC states that PG&E neither confirms nor denies culpability for the infractions. With its near-bankruptcy failure to deal with

---

<sup>7</sup> "Digital 'timebomb' discovered in devices worldwide", ,Blake Sobczak, E&E News, published: Thursday, May 24, 2018

<sup>8</sup> Docket No. RM16-18-000, Cyber Systems in Control Centers (Issued July 21, 2016)



an energy supply conspiracy a decade ago<sup>9</sup>, and the San Bruno gas pipeline explosion costing 8 fatalities (including failure to admit to gas leaks to the NSTB)<sup>10</sup>, PG&E's reluctance to be identified with this 2016 data breach is understandable. But it should not be allowed in the interest of its customers and investors. Furthermore, the PG&E contractor should also be identified if there would ever be a "lessons-learned" from this affair. The NP filing fails to state whether the vendor is still under contract or if it has been blacklisted by PG&E or the WECC.

## Legal and Regulatory Concerns

### *Contractual Relationships*

At this point, this major event is not deserving of Critical Energy Infrastructure Information (CEII) protection. The damage has, long since, been catalogued by the nation's adversaries. The gaps in public understanding of this event should be closed. Was the development effort a new contract or a continuing one? If the latter, what were the security provisions governing vendor actions? PG&E's actions? How did they conform to CIP standards? When was this contract entered into? Were there any provisions in the continuing contract that were major factors in the settlement negotiations? If there were, and they put PG&E's cyber assets or operations in harm's way (in retrospect) how far back in time did they extend? If this was a continuing contract, it's important to understand the nature of security vulnerabilities, both at PG&E and at its vendor, and how far back in time they extend.

If it was a new contract, did the contractor have PG&E's permission to access the Asset Database (hereafter "DB") on-line, across the Internet? If so, was that access through secure means or "*en clair*"? Did the contractor have PG&E's permission to download the DB? If so, what restrictions were applied by PG&E? If the contractor did not have permission to take possession of the DB, that was potentially a criminal act. In that event, was it reported to California authorities, to the FBI? If not, why not? If any PG&E authority gave permission for

---

<sup>9</sup> California State Senate Energy, Utilities and Communications; Background Relative to Bankruptcy Proceedings, PG&E Bankruptcy Filing, April 6, 2001

<sup>10</sup> Prosecution rests its case in PG&E's federal criminal trial, Mercury News By George Avalos | gavalos@bayareanewsgroup.com

the downloading, that should be reported along with the corrective action taken by PG&E. The entire investigation should have been documented in the settlement and in the NERC NP, unless embargoed as part of a criminal investigation.

### ***CIP Standards***

Events of the last several years have conflated several important CIP Standards issues, notably Communications between Control Stations, Incident Reporting vs. malware extraction, and Supply Chain vulnerabilities. Efforts by FERC and NERC to deal with these separately have failed; the interrelationships are too complex. Isologic LLC, Resilient Societies, and Applied Control Solutions, LLC petitioned FERC to reopen the evidentiary record on Order No. 822 following the 2014 Russian incursion in the US Grid and the 2015 follow-on attack on the Ukrainian Grid.<sup>11</sup> That request was denied by FERC<sup>12</sup> but led to issuance of Order No. 829 to address intercommunications between control stations (including Internet connectivity). The latter issue links into vendor-utility relationships. The CIP 002-5.1a exclusion of communications and networks from CIP standards is a huge impediment to management of vendor and supply chain vulnerabilities, to say nothing about vendor- support to BES substations industrial control systems (ICS). If this absurdity is not fixed, there is no hope for protection of cyber assets.

PG&E interactions with its vendor are, of course, grist for their contractual relationships. The vendor has already paid some price for his actions, but PG&E would certainly have benefited in the settlement if there existed a hard CIP standards requirement that specifically held the utility responsible for controlling the electronic interfaces with vendors; thereby almost certainly to be addressed in contracting. NERC will argue that CIP 003-7 essentially does this, but it really doesn't. Isologic LLC and Resilient Societies have recommended<sup>13</sup> blacklisting, whitelisting and independent third party security evaluations relative to supply chain vulnerabilities; essentially ignored to now by FERC.

---

<sup>11</sup> Filings of March 29, 2016, seeking reopening of the record supporting FERC Order No. 822.

<sup>12</sup> North American Electric Reliability Corporation Docket No. RR15-2-005 Order on Compliance Filing (Issued Nov 16, 2016).

<sup>13</sup> Isologic LLC Filing on NOPR Supply Chain Risk Management Reliability Standards, [Docket No. RM17-13-000] (January 18, 2018) .

Throughout 2016 and 2017, several NERC SDT's developed proposals addressing issues in FERC Order No. 829, proposals that are still open FERC actions, including CIP 003-7. Were those Standard Drafting Teams (SDT's) made aware of the PG&E CIP violations, if not, why not? NERC was most certainly aware of the event and the direct relationship to Order No. 829 tasks. To what extent did NERC seek FERC guidance on "lessons learned" from the PG&E negotiations?

### ***The 2016 CMEP Report***

A review of the Compliance Monitoring Enforcement Program (CMEP) report for 2016<sup>14</sup> fails to highlight the extraordinary facts of the PG&E event. Admittedly the annual report is a statistical and anonymous summary, but it does cite major violations and regulatory infractions and should have alluded to this event, as one means of keeping utilities seriously engaged in compliance. For the past several years, security incidents occurring on the North American Grid have been suppressed despite a clear DOE requirement<sup>15</sup> to file OE-417 reports on any incident that has the potential to disrupt the BES. The May 2016 PG&E incident certainly qualified but it was not entered. And this NP studiously avoids that issue. NERC continues its push for non-public reporting of industry infractions in its Reliability Assurance Initiative (RAI) program, the latest being a proposed extension of self-reported medium risk violations as Compliance Exceptions (CEs).<sup>16</sup> The proposal has been denied by FERC but the misuse of CEI, if that is present in this event, needs to be addressed.

### **Assessment of Risk to the Bulk Electric System**

Not unexpectedly, the limited facts of the event promulgated by PG&E and the WECC assessment of BES risk reflect understatement, minimization of details, misstatements and corrections, and serious mischaracterization and omission of vulnerabilities. Along with almost zero inclusion of ongoing threats to PG&E cyber assets, and by extension, much broader threats to other utilities in the Western Interconnection, the Public Utility Commissions of California,

---

<sup>14</sup> North American Electric Reliability Corporation's annual compliance monitoring and enforcement program filing, Docket No. RR15-2-000 February 21, 2017

<sup>15</sup> OE-417 Electric Emergency Incident and Disturbance Report, Revised November 2014

<sup>16</sup> NERC CMEP for 2016, Docket No. RR15-2-000 February 21, 2017

the clients for PG&E, the National Security installations on the West Coast are significantly put at risk. Risk to the BES spells risk to the Distribution systems serving major urban areas, industries other than the electric utilities, other critical infrastructures of the region. It is simply incredible that the WECC would state the duration of the infraction as 590 days, and yet conclude that there was low likelihood that the massive data breach was accessed by other than the security researcher. The breach included over 680,000 log entries; a gold mine for adversarial analysis. Did PG&E or WECC contact DHS/US CERT for assistance on forensics or the overall security assessment?

The timing is equally important. During 2015/2016 and continuing into 2017, while the PG&E event was transpiring, Russian SVR(Foreign Intelligence) and Russian Ministry of Defense (MOD)/GRU (Military Intelligence) actors were busy exploiting our 2016 national election while continuing its extensive reconnaissance (and worse) in the North American Grid. Exploitation and development of destructive tools occurred, with testing of Russian malware improvements in the Ukrainian Grid in 2015 and 2016. Yet a proposed CIP standard requiring removal of known malware was opposed by NERC and others.<sup>17</sup>

There is literally no way to ensure that the exposure of the PG&E asset database has not been exploited by Russian cyber forces. They have demonstrated mastery of reconnaissance, surreptitious entry, modification of software and firmware, an ability to withdraw without leaving traces of their presence. They have shown they can exploit supply chains, deep in system development; capabilities to understand and modify control systems, a deep knowledge of industrial control systems and their vulnerabilities.<sup>18</sup> Those who would undertake assessments of such incidents should study these threats, their flexibility, and their ultimate goals. The simple admission of “Risk” does not do justice to the topic.

The PG&E extended security evaluation left many gaps. The entire flow, every communications node, multiple networks and servers, programmable interfaces, storage systems and all

---

<sup>17</sup> NERC Comments, Cyber Security Incident Reporting Reliability Standards Docket Nos. RM18-2-000 AD17-9-000, February 26, 2018

<sup>18</sup> See for example, ESET Research Report, “Sednit adds two zero-day exploits using ‘Trump’s attack on Syria’ as a decoy” ESET Research 9 May 2017 - 08:00PM

personnel accesses should have been analyzed to reliably document the violations. Only in this way would it be possible to identify leakages, opportunities for exploitation, and need for standards improvement. There needed to be collection of every access to the network and storage systems holding asset data. There needed to be rigorous examination against holdings of Grizzly Steppe and other intelligence on Russian intrusions in US systems, both Grid and other infrastructure. For the risks are not just to the BES, but to the entire nation. The WECC and PG&E assessment was far from a cover-up but given the events of the past three-four years, it was decidedly myopic.

## **FERC's Fiduciary Responsibilities to Assist the Several States in Reforming a Culture of Physical-Cyber Insecurity Tolerance**

We wish to remind especially the newly-serving FERC Commissioners that the Critical Infrastructure Protection (CIP) reliability standards are mandatory for registered entities in the bulk electric system, but generally are only advisory within electric distribution entities serving the several states. The states have their own need to strengthen cybersecurity. And helping the states attain these goals is also essential for improved physical-cybersecurity of the bulk electric system. FERC Commissioners need only look to what happened in the Ukrainian grid during December 2015 and December 2016. Foreign actors, operating from remote systems within Russia, entered the Ukrainian distribution system operator control systems, which also provided cyber entry pathways back to regional transmission and control systems.

If FERC determines to provide *fig leaf cover* for the largest gas-electric utility in the State of California, by averting formal acknowledgment that the presently Unidentified Registered Entity (URE) is in fact Pacific Gas & Electric Corporation, and by identifying the unnamed Contractor-Vendor materially responsible for the resulting hazards, how will the California Public Utilities Commission change the business-as-usual culture that places at risk the entire system operated through the California Independent System Operator and the entire Western Interconnection?

## **Initiatives of the California Public Utilities Commission Deserving FERC Support**

On August 27, 2015 the California Public Utilities Commission (hereafter “CPUC”) which regulates gas and electric services of Pacific Gas & Electric Corporation within California, commenced a formal investigation:

**“into whether the organizational culture and governance of PG&E Corporation and the Utility prioritize safety and adequately direct resources to promote accountability and achieve safety needs and standards...”**

PG&E has been fined \$2.25 billion -- three orders of magnitude more than the proposed cyber-security fine announced on February 28, 2018 -- for deaths, fires, and a failure of accountability linked to the San Bruno pipeline fire. Further, in April 2013, the Metcalf Substation shootout of 17 high voltage transformers was ascribed by PG&E spokespersons as mere “vandalism.”

Following a preliminary investigation by the California PUC (CPUC), both by an internal CPUC staff unit and by a designated monitor, on May 8, 2017 the CPUC released the Consultant’s report, with a scoping memo proposing a second stage of investigation of the operating culture within PG&E Corporation. Further, the CPUC “will evaluate the safety recommendations of the consultant... The scoping memo will also consider all necessary measures, including but not limited to, a potential reduction of the Utility’s return on equity until any recommendations adopted by the CPUC are implemented ....”

One of the remaining issues in dispute, after PG&E and the CPUC agreed on several findings and recommendations, was and remains “cyber security.”<sup>19</sup>

Hence, if FERC proceeds to conceal the name of the Unidentified Registered Entity to be fined merely \$2.7 million as of February 28, 2018,<sup>20</sup> the California PUC Staff will know who failed

---

<sup>19</sup> PG&E Corporation, Form 10-Q for the Quarterly Period ended March 31, 2018, Part II, Item 1 (“Legal Proceedings”), filed with the SEC May 3, 2018, available online via the SEC’s EDGAR database.

<sup>20</sup> Relying upon the latest 10-Q financial statement from PG&E Corporation, the net assets of the PG&E Corporation, after subtracting outstanding liabilities, as of March 31, 2018 were \$19.983 Billion dollars. So a fine of

California ratepayers and citizens, but it will not receive formal, public notice of these hazards. It will receive less than minimal support from FERC to change a culture of “business as usual” disregard of protective standards, not intentional disregard, but complacency, and false claims of a “fake” database being at risk” and an undetected infrastructure exposure that apparently lasted as long as 590 consecutive days before exposure, not by PG&E but by an independent “white hat” cyber specialist.

## Conclusion and Recommendations

The proposed settlement should not be accepted by FERC. The penalty is less than one-tenth of one percent of PG&E’s operating income for 2017,<sup>21</sup> and far less of the corporation’s net worth. This penalty is hardly enough for the wake-up call this data breach deserves.<sup>22</sup> The Commission will probably conclude that no useful purpose would be served by a larger penalty, but much is in turmoil in the Western Interconnection:

At least three separate organizations are claiming responsibility as the Western Interconnection Regional Reliability Coordinator, the WECC that lost the job several years ago, Peak RC facing the loss of member PG&E, and CAISO (with PG&E as its cornerstone.)

- The loss of the Canadian Province of Alberta to the Western Interconnection.

---

merely \$2.7 million dollars is just 1.35 thousandth of one percent of the net equity of the firm. A fine so minimal, particularly with the benefits of FERC-sponsored anonymity, would be an invitation to future safety, reliability, and security impunity by PG&E and its vendors.

<sup>21</sup> PG&E 2017 Revenue: \$17.14B, Operating Income \$2.96B, Net Income \$1.66B, SEC Annual Report 2017

<sup>22</sup> Although PG&E was not the original source of the system wide compromise, that corporation was reckless in failing to monitor its vendor’s practices, willful in claiming the compromised database was “fake,” and tardy in its responsive actions. When there has been reckless behavior resulting in harm, punitive damages are widely assessed in civil tort actions. See the following literature: Robert D. Cooter, “Economic Analysis of Punitive Damages,” 56 *S. Cal. L. Rev.* 79 (1982); K. S. Abraham and J. C. Jeffries, “Punitive damages and the rule of law: the role of defendant’s wealth,” 18 *J. Legal Studies* 415 (1989); S. M. Polinsky and S. Shavell, “Punitive Damages: An Economic Analysis,” 111 *Harv. L. Rev.* 869 (1998); Note, “Common Sense Legislation: The Birth of Neoclassical Tort Reform,” 109 *Harv. L. Rev.* 1765 (1996); N. R. Mead, “Who is liable for insecure systems?” 37 *Computer*, July 2004, 27-34; I. B. Utne, et al. “A method for risk modeling of interdependencies in critical infrastructure,” *Reliability Engineering & System Safety*, 2011, v. 96, 671-678; Chee-Woo Ten, et al. “Impact assessment of Hypothesized Cyberattacks on Interconnected Bulk Power systems,” *IEEE Trans. Smart Grid*, Jan. 2017

- The contemplated defection of the Southwest Power Pool (SPP) from the Eastern Interconnection in favor of a partnership with Mountain West Transmission Group Initiative.
- A potential partnership between PEAK RC and a unit of PJM with the same objective.
- And a declaration by PG&E's CAISO of intention to compete for RTO control as well.

FERC's authorities in these efforts are apparently being ignored. But what is the effect of all of this on Grid Reliability, and its stepchild Cybersecurity? Not good to say the least. This Notice of Proposed Penalty without a significant upgrading of the fine and public identification of the Unidentified Registered Entity and its Contractor-Vendor will reinforce the sense of impunity to the foregoing participants. FERC should not let that happen.

We note with regret that in response to a third party FOIA request,<sup>23</sup> FERC has as recently on May 25, 2018 claimed that the Unidentified Responsible Entity (URE) should be shielded from disclosure as a matter of protecting Critical Energy Infrastructure Information. We understand the CEII protection through completion of review by the FERC Commissioners. But if FERC continues to shield the URE and its Contractor-Vendor and agrees to a fine that is miniscule in relation to annual operating income or equitable net worth as high as \$19.983 billion dollars, we would propose an alternative acronym: Critical Energy Impunity Inducement, also CEII.

Despite loss of two years, FERC should create a joint FERC-DOE-FBI team to comprehensively review the PG&E event. That study should address the real-world facts of potential compromise, interview the security researcher who made the initial report, investigate any linkages to Russian incursions in the North American Grid, make recommendations on changes to reliability and cybersecurity standards arising out of the investigation, and validate or revise a penalty amount recommendation to FERC.

We respectfully request the FERC Commissioners signal the benefits of transparency, impose a significantly higher penalty, publicly identify the Unidentified Responsible Entity, publicly identify the Unidentified Contractor-Vendor, and request a FERC, DOE, and FBI joint

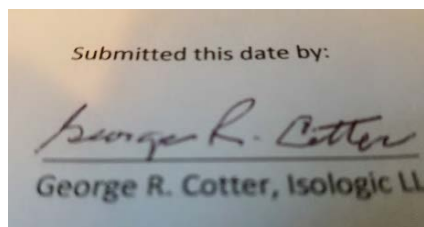
---

<sup>23</sup> Michael Mabee. FERC Response and denial dated May 25, 2018.



investigation to determine whether adversary actors have acquired access to the asset and communications linked Data Base at risk for approximately 590 consecutive days in years 2015-2017.

Respectfully submitted,



Submitted this date by:  
*George R. Cotter*  
George R. Cotter, Isologic LLC

Respectfully submitted by:



Thomas S. Popik, Chairman,



William R. Harris, Secretary,

For the

**Foundation for Resilient Societies**

52 Technology Way

Nashua, NH 03060-3245

[www.resilientsocieties.org](http://www.resilientsocieties.org)

[williamh@resilientsocieties.org](mailto:williamh@resilientsocieties.org)

Document Content(s)

NP18-7-000 Joint Isologic & Resilient\_Societies Comments.PDF.....1-16

**Exhibit F**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**



## CENTER FOR SECURITY POLICY

Frank J. Gaffney, Jr., President & CEO

29 May 2018

Chairman Kevin J. McIntyre  
Commissioner Neil Chatterjee  
Commissioner Cheryl A. LaFleur  
Commissioner Robert F. Powelson  
Commissioner Richard Glick  
Federal Energy Regulatory Commission  
888 First Street, NE  
Washington, DC 20426

### **Comments submitted in FERC Docket NP18-7-000 on a Notice of Penalty for an Unidentified Registered Entity**

Dear Chairman McIntyre, Commissioner Chatterjee, Commissioner LaFleur, Commissioner Powelson, and Commissioner Glick:

After serving in the Reagan administration in various positions, including acting as the Assistant Secretary of Defense for International Security Policy, I founded the Center for Security Policy – a not-for-profit, non-partisan educational corporation which strives to provide timely, informed analyses and recommendations concerning critical foreign and defense policy challenges.

Among the most critical of those challenges are the various, looming threats to America’s electric grid. Consequently, from the time of the Commission on the Electromagnetic Pulse (EMP) Threat’s first report to Congress in 2004 to the present day, the Center – like many other leaders in the national security arena – have been warning that the grid’s lack of resilience poses a potentially existential danger to our country.

As you know, this vulnerability can be exploited by enemies using a variety of techniques including physical sabotage, electromagnetic attack, or cyberattack. Given that the very survival of our nation depends upon the protection of grid assets against these forms of attack, there is great public interest in doing so.

During the comment period for Docket RM18-2-000 on Cyber Incident Reporting, our organization argued that it is necessary that the Federal Energy Regulatory Commission (“FERC” or “the Commission”) order NERC to set an enhanced standard for malware detection, reporting, mitigation, and removal. This commonsense recommendation – which was vehemently opposed by others on the docket, including many in the electric utility industry who claimed such a standard would be “unduly burdensome” and “unnecessary” – was apparently unpersuasive to FERC since no such enhanced standard has been established to date.

Even though FERC has the authority under Section 215(d)(5) of the Federal Power Act to order a proposed reliability standard to address the yawning gaps in the current NERC cybersecurity policy, it “declined to propose” additional Reliability Standard measures, to the potentially severe detriment to our national security and the safety of hundreds of millions of Americans.

During our organization’s comments for Docket RM18-2-000, we listed ample evidence from the public domain pointing to the rapidly increasing risk of malware present in information technology (IT) and operational technology (OT) associated with electric grid infrastructure, posing a grave and immediate danger to the American people who depend on this infrastructure for daily life. Even since the time of our previous comments in February 2018, more has been learned about the incredible effectiveness of Russian SVR (Foreign Intelligence) and Russian Ministry of Defense (MOD)/GRU (Military Intelligence) actors’ reconnaissance of U.S. grid IT systems; surreptitious penetration of those systems; modification of software and firmware; and ability clandestinely to withdraw without a trace.

As recently as March of this year, the U.S. Department of Justice reported that your own Commission was the target of a massive cyber operation orchestrated by the Islamic Republic of Iran to steal information from governments and private companies worldwide.

Meanwhile, as you well know, at the same time as these adversaries of our nation were busy penetrating the cyber systems of our government and private energy industry, one of our nation’s largest utilities unwittingly allowed a massive 590-day data breach, including 680,000 log entries, violating Security Management standards specified in CIP 003-3 Requirement R4 (*implement a program to identify, classify and protect information associated with CCA assets*) and Requirement R5 (*implement a program for controlling access to CCA information*) and putting the National Security installations on the West Coast of America at risk – to say nothing of major urban areas and private corporations working in Silicon Valley. This very same utility suffered one of the most renowned and frightening physical attacks on its infrastructure in April 2013. And a year later, in 2014, it failed to keep thieves from stealing assets within the previously targeted substation, possibly encouraged by the utility’s suggestion that the previous penetration of their infrastructure was mere “vandalism.”

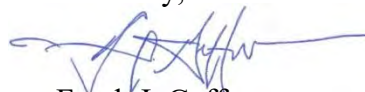
Incredibly, despite the Western Electricity Coordinating Council concluding that the cyber security violation posed a severe risk to the Bulk Electric system (“BES”) and the assessment of a \$2.7M penalty, your commission seems disinclined to identify this utility and its offending contractor, contrary to the clear interests of its customers and investors and the public at large. As such, not only does FERC deny the opportunity for “lessons learned” to be shared among other utilities, it signals to the owners and operators of our nation’s most critical infrastructure that the “business as usual” culture of lackadaisical security can remain in place for our adversaries to exploit.

With Docket NP18-7-000 and its Notice of Penalty for an Unidentified Registered Entity, FERC has the opportunity to be transparent about this dangerous cyber security breach, and publicly identify the currently “Unidentified Responsible Entity” and “Unidentified Contractor-Vendor.” As an agency of the Federal Government, FERC has the power to request a joint investigation

with other Federal Agencies to help both determine adversarial access to the utility's system and to inform future cyber security policies of the U.S. Government and private industry.

The Center for Security Policy once again calls on you to exercise your authority to require clearly necessary enhancements of the U.S. electric grid's resiliency to cyber and other forms of man-induced and naturally occurring threats. To do otherwise is to be complicit in the reckless perpetuation of grave dangers to the public safety and national security.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Frank J. Gaffney', with a long horizontal flourish extending to the right.

Frank J. Gaffney  
President and CEO

cc: Hon. Rick Perry, Secretary of Energy

Document Content(s)

FrankGaffney-FERC-DocketNP18-7-000.PDF.....1-3

**Exhibit G**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**



163 FERC ¶ 61,153  
UNITED STATES OF AMERICA  
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation

Docket Nos. NP18-10-000  
NP18-7-000

NOTICE

(Issued May 30, 2018)

Take notice that the Commission will not further review, on its own motion, the following Notices of Penalty:

<u>Docket No.</u>	<u>Filing Date</u>	<u>Registered Entity</u>
NP18-10-000	April 30, 2018	Spreadsheet NOP

In addition, pursuant to 18 C.F.R. §39.7(e)(1) (2012), 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.

If no further action is taken by the Commission in this matter by that date, the penalties will be deemed affirmed by operation of law.

By direction of the Commission.

Nathaniel J. Davis, Sr.,  
Deputy Secretary.

Document Content(s)

NP18-10-000.DOCX.....1-1

**Exhibit H**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

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).<sup>1</sup> 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.<sup>2</sup>

---

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

<sup>2</sup> 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 information<sup>3</sup>. 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.<sup>4</sup> Disclosure of the requested information is critical to the public's understanding of how

---

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

<sup>4</sup> 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.<sup>5</sup> 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:”

---

<sup>5</sup> 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](mailto:CivilDefenseBook@gmail.com).

Sincerely,

A handwritten signature in blue ink, appearing to read 'ML' or similar initials, with a flourish at the end.

Michael Mabee

**Exhibit I**  
**To Petition for Rulemaking**  
**Submitted by 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](mailto:edwin.kichline@nerc.net)

Dear Mr. Kichline:

Pursuant to the Freedom of Information Act (FOIA)<sup>1</sup> 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".

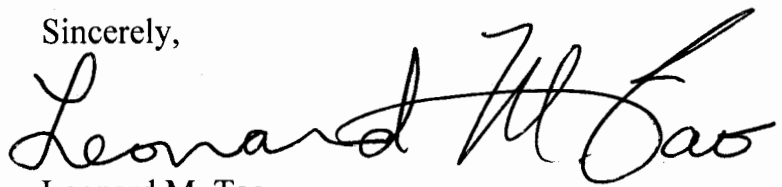
Because your company has asserted a privileged and confidential interest in the information requested, we are soliciting your comments on whether release of the information is required under the FOIA. Your written comments are due within five business days from the date of this letter, and should clearly 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](mailto:foia-ceii@ferc.gov).

---

<sup>1</sup> 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, reading "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 solid black rectangular redaction box covering several lines of text.

[CivilDefenseBook@gmail.com](mailto:CivilDefenseBook@gmail.com)

**Exhibit J**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

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

**Exhibit K**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

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)<sup>1</sup>, 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.

---

<sup>1</sup> 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 documents<sup>2</sup> 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.<sup>3</sup>

*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).

---

<sup>2</sup> 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.

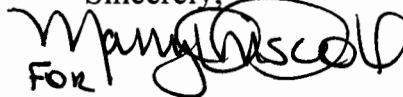
<sup>3</sup> CEII is specifically exempted from disclosure under the Fixing America's Surface Transportation Act, Pub. L. No. 118-94, § 61003 (2015) (establishing applicability of FOIA Exemption 3, 5 U.S.C. 552(b)(3) (protecting material specifically exempted by statute).



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](mailto: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

**Exhibit L**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

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.<sup>1</sup> 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).<sup>2</sup> I am not seeking any CEII. I simply ask for disclosure

---

<sup>1</sup> 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.

<sup>2</sup> 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.<sup>3</sup>

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](mailto:CivilDefenseBook@gmail.com).

Sincerely,



Michael Mabee

Attachments

CC: Charles A. Beamon, Associate General Counsel  
Via Email: [charles.beamon@ferc.gov](mailto:charles.beamon@ferc.gov)

---

<sup>3</sup> 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).

**Exhibit M**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

FEDERAL ENERGY REGULATORY COMMISSION

WASHINGTON, D. C. 20426

AUG - 2 2018

OFFICE OF THE GENERAL COUNSEL

Re: Freedom of Information Act  
Appeal, FOIA No. FY18-75

**VIA E-MAIL AND CERTIFIED MAIL**

Michael Mabee (without enclosures)



CivilDefenseBook@gmail.com

Dear Mr. Mabee:

This letter responds to your correspondence received on June 16, 2018, in which you appealed the May 25, 2018 denial of your request filed pursuant to the Freedom of Information Act (FOIA) and the Federal Energy Regulatory Commission's (Commission) FOIA regulations. 5 U.S.C. § 552, *as amended* by the FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 (2016); 18 C.F.R. § 388.108 (2018).

On April 13, 2018, you requested the following:

1. 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.<sup>1</sup>
2. correspondence between FERC and NERC laying out any purported rationale for withholding the identity 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 cited certain Commission orders.

---

<sup>1</sup> Your request was not construed to seek the February 28, 2018 NERC Full Notice of Penalty itself.

On May 25, 2018, Leonard M. Tao, Director of the Office of External Affairs (Director), determined that the seven (7) responsive documents<sup>2</sup> were protected from disclosure in their entirety pursuant to FOIA Exemptions 3 and 7(F), and therefore, denied your request. By letter dated June 16, 2018, you appealed that determination. Specifically, you argue that you are not seeking Critical Energy/Electric Infrastructure Information (CEII) and that you “simply ask for disclosure of the identity of the ‘Unidentified Registered Entity’ [URE] and why this information has been withheld.”

FOIA Exemption 3 protects information “specifically exempted from disclosure by statute.” Here, CEII is specifically exempted from disclosure under the Fixing America’s Surface Transportation Act, Pub. L. No. 118-94, § 61003 (2015). I conclude that the responsive documents contain sensitive cyber security-related information that qualifies for protection as CEII, and thus, was appropriately withheld. See 18 C.F.R. § 388.113(c). FOIA Exemption 7(F), 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).<sup>3</sup> In this regard, the requested documents contain information regarding cyber security and risks to the URE, as well the techniques used to resolve the incident and associated possible vulnerabilities, the disclosure of which could provide a potential bad actor with information that may assist it in targeting the entity for cyber intrusion attacks. See *Public Employees for Environmental Responsibility, U.S. Section, Int’l Boundary and Water Comm.*, 740 F.3d 195, 206 (D.C. Cir. 2014) (Exemption 7(F) protects “the many potential threats posed by the release of sensitive agency information.”). Therefore, the Director also correctly invoked FOIA Exemption 7(F) to withhold the relevant documents.

While it is possible that the name of a URE may constitute CEII under 18 C.F.R. 388.113 and qualify for protection under Exemption 7(F), under the circumstances and facts presented in this particular case, I conclude that the name of the URE can be disclosed. However, other information contained in the documents which I conclude should remain protected under Exemptions 3 and 7 has been redacted. Additionally, the names of lower-level employees have been redacted pursuant to FOIA Exemption 6. See

---

<sup>2</sup> These documents consist of various email correspondence between FERC and NERC regarding questions concerning details relative to the incident resulting in the Notice of Penalty.

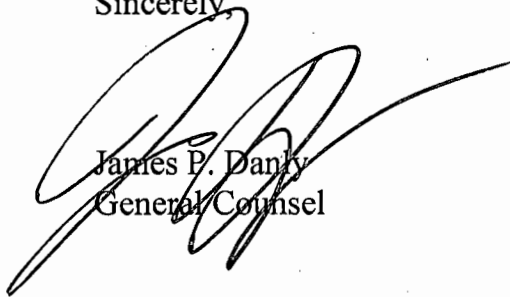
<sup>3</sup> I note that Exemption 7(F) applies to civil, as well as criminal law enforcement matters. See *Vento v. IRS*, 714 F. Supp. 2d 137, 148 (D.D.C. 2010) (holding that distinguishing between civil and criminal enforcement is incorrect because there “is no warrant in the law for that distinction and the federal courts have rejected it.”)

*Judicial Watch, Inc. v. Bd. of Governors of Fed. Reserve System*, 773 F. Supp. 2d 57, 62 (D.D.C. 2011); *see also Elec. Privacy Info. Ctr. v. Dep't of Homeland Sec.*, 384 F. Supp. 2d 100 (D.D.C. 2005) and *Cofield v. City of LaGrange, Ga.*, 913 F. Supp. 608, 616 (D.D.C. 1996).

Accordingly, your appeal is granted in part and denied in part. This letter also constitutes notice to NERC that this information will be made available to you no sooner than five (5) calendar days from the date of this letter. *See* 18 C.F.R. § 388.112(e).

Judicial review of this decision is available to you in the United States District Court for the judicial district in which you live, or in the United States District Court for the District of Columbia, which would be the location of the data that you seek. You may also seek mediation from the Office of Government Information Services (OGIS). Using OGIS services does not affect your right to pursue litigation. 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](mailto:ogis@nara.gov); telephone at (301) 837-1996; facsimile at (301) 837-0348; or toll-free at 1-(877) 684-6448.

Sincerely,



James P. Dandy  
General Counsel

**Via Email**

Edwin G. Kichline (with enclosures)  
Senior Counsel and Director of  
Enforcement Oversight  
North American Electric Reliability Corporation  
1325 G Street N.W. Suite 600  
Washington, D.C. 20005  
[edwin.kichline@nerc.net](mailto:edwin.kichline@nerc.net)



**Exhibit N**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

Federal Energy Regulatory Commission  
Washington, DC 20426

AUG 24 2018

Re: Freedom of Information Act  
Appeal, FOIA No. FY18-75

**VIA E-MAIL AND CERTIFIED MAIL**

Michael Mabee

[REDACTED]

[REDACTED]

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

This letter concerns your June 16, 2018 appeal pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552 and the Federal Energy Regulatory Commission's (Commission or FERC) FOIA regulations, 18 C.F.R. § 388.110 (2018). You appealed the decision issued on May 25, 2018 by Leonard M. Tao, Director of the Office of External Affairs (Director), which withheld the requested documents under FOIA Exemptions 3 and 7(F).

By letter dated August 2, 2018, General Counsel James P. Danly granted in part, and denied in part your appeal and determined to release the documents in redacted form. The General Counsel's decision also provided notice to the submitter that parts of the requested documents would be released no sooner than five (5) calendar days after the issuance of his decision pursuant to 18 C.F.R. § 388.112(e). Accordingly, the redacted versions of the documents are enclosed.

Sincerely,



Charles A. Beamon  
Associate General Counsel  
General & Administrative Law

Enclosures

**David Ortiz**

---

**From:** Robert Chambers  
**Sent:** Friday, March 30, 2018 12:00 PM  
**To:** David Ortiz; [REDACTED]; Mark Hegerle; Olutayo Oyelade [REDACTED]; [REDACTED]  
**Cc:** Loye Hull; [REDACTED]  
**Subject:** FW: NP18-7 questions

FYI...

**From:** Robert Chambers  
**Sent:** Friday, March 30, 2018 11:58 AM  
**To:** 'Leigh Anne Faugust' <Leigh.Faugust@nerc.net>  
**Cc:** Ed Kichline (Ed.Kichline@nerc.net) <Ed.Kichline@nerc.net>; Loye Hull <loye.hull@ferc.gov>; [REDACTED]  
**Subject:** NP18-7 questions

We have some questions regarding the full NOP, NP18-7:

Redacted pursuant to FOIA Exemptions 3 and 7

**Risk Analysis**

[REDACTED]

- [REDACTED]

[REDACTED]

- **The Stipulated Incident Facts state** [REDACTED]

- [REDACTED]

- [REDACTED]

**Mitigation of Risk**

In the URE mitigation plan, the plan detail section states

[REDACTED]

[REDACTED]

[REDACTED]

The Stipulated Incident Facts state [

[REDACTED]

Name (@pge.com),

Domain

[REDACTED]

- [REDACTED]

- **If so, please describe and explain the analysis performed and the detailed results.**

- [REDACTED]

- [REDACTED]

- [REDACTED]

Please provide your response on or before April 16, 2018.

Thank you,

**Bob Chambers**  
**Manager – Security Group 1**  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-665-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. All information herein contains staff pre-decisional deliberations, privileged or confidential, commercial, or financial information, and/or critical energy infrastructure information and is not for public release. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and do not reflect those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.

**From:** Robert Chambers  
**To:** Cynthia Pointer  
**Cc:** Kal Ayoub (kal.ayoub@ferc.gov)  
**Subject:** FW: NP18-7 questions  
**Date:** Thursday, April 05, 2018 5:09:00 PM

---

FYI...

Redacted pursuant to FOIA Exemption 6

**From:** Robert Chambers  
**Sent:** Monday, April 02, 2018 7:43 AM  
**To:** 'Ed Kichline' <Ed.Kichline@nerc.net>; Leigh Anne Faugust <Leigh.Faugust@nerc.net>  
**Cc:** Loye Hull <loye.hull@ferc.gov>; [REDACTED]  
**Subject:** RE: NP13-7 questions

Good morning Ed,

If that is possible in the future, we will let you know...

**Bob Chambers**  
**Manager – Security Group 1**  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-665-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

**From:** Ed Kichline [<mailto:Ed.Kichline@nerc.net>]  
**Sent:** Friday, March 30, 2018 1:28 PM  
**To:** Robert Chambers <[Robert.Chambers@ferc.gov](mailto:Robert.Chambers@ferc.gov)>; Leigh Anne Faugust <[Leigh.Faugust@nerc.net](mailto:Leigh.Faugust@nerc.net)>  
**Cc:** Loye Hull <[Loye.Hull@ferc.gov](mailto:Loye.Hull@ferc.gov)>; [REDACTED]  
**Subject:** RE: NP18-7 questions

Bob,

We will send these questions to WECC to start working along with the registered entity on the responses.

Loye had indicated in early March that there might be questions on the Full NOP. If possible in future months, we would appreciate if you could let us know that it is likely the Commission will extend its period for review prior to issuance of the Commission's Notice. That can help us keep the Regional Entity, the registered entity, and our management informed and result in less alarm when there is a Notice of Further Review.



- The Stipulated Incident Facts state [REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

**Mitigation of Risk**

In the URE mitigation plan, the plan detail section states [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]

The Stipulated Incident Facts state [REDACTED]  
[REDACTED]  
[REDACTED]  
*Domain Name (@pge.com)*  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]



- **If so, please describe and explain the analysis performed and the detailed results.**

- [Redacted]
- [Redacted]
- [Redacted]

Please provide your response on or before April 16, 2018.

Thank you,

**Bob Chambers**  
Manager – Security Group 1  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-665-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. All information herein contains staff pre-decisional deliberations, privileged or confidential, commercial, or financial information, and/or critical energy infrastructure information and is not for public release. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and do not reflect those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.

Warning: This email comes from an external sender. Be cautious when opening URLs or attachments from external senders.

CP

**From:** Robert Chambers  
**To:** David Ortiz [redacted]; Mark Hegerle; Olutayo Oyelade: [redacted]  
**Cc:** Loye Hull; [redacted] a  
**Subject:** FW: NP18-7 questions  
**Date:** Friday, March 30, 2018 12:00:14 PM

---

FYI...

**From:** Robert Chambers  
**Sent:** Friday, March 30, 2018 11:58 AM  
**To:** 'Leigh Anne Faugust' <Leigh.Faugust@nerc.net>  
**Cc:** Ed Kichline (Ed.Kichline@nerc.net) <Ed.Kichline@nerc.net>; Loye Hull <loye.hull@ferc.gov>; [redacted]  
**Subject:** NP18-7 questions

We have some questions regarding the full NOP, NP18-7:

**Risk Analysis**

Redacted pursuant to FOIA Exemptions 3 and 7

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

- **The Stipulated Incident Facts state** [redacted]

- [redacted]

- [redacted]

[REDACTED]  
[REDACTED]?

**Mitigation of Risk**

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

• [REDACTED]  
[REDACTED]  
[REDACTED]

• [REDACTED]  
[REDACTED]

The Stipulated Incident Facts state [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED] *Domain Name (@pge.com)*, [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

• [REDACTED]  
[REDACTED]  
[REDACTED]

• **If so, please describe and explain the analysis performed and the detailed results.**

• [REDACTED]  
[REDACTED]  
[REDACTED]

• [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]

Please provide your response on or before April 16, 2018.

Thank you,

**Bob Chambers**  
**Manager – Security Group 1**  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-865-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. All information herein contains staff pre-decisional deliberations, privileged or confidential, commercial, or financial information, and/or critical energy infrastructure information and is not for public release. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and do not reflect those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.

4/14/2018

Mail - Kai.Ayoub@ferc.gov

# FW: NP18-7 questions

Robert Chambers

Redacted pursuant to FOIA Exemption 6

Fri 3/30/2018 12:00 PM

To: David Ortiz <David.Ortiz@ferc.gov>; [REDACTED] Mark Hegerle <Mark.Hegerle@ferc.gov>;  
Olutayo Oyelade <Olutayo.Oyelade@ferc.gov>; Michael Keane <Michael.Keane@ferc.gov>; Barry Kuehnle <Barry.Kuehnle@ferc.gov>;  
[REDACTED]

Cc: Loye Hull <Loye.Hull@ferc.gov>; [REDACTED]

FYI...

From: Robert Chambers  
Sent: Friday, March 30, 2018 11:58 AM  
To: 'Leigh Anne Faugust' <Leigh.Faugust@nerc.net>  
Cc: Ed Kichline (Ed.Kichline@nerc.net) <Ed.Kichline@nerc.net>; Loye Hull <loye.hull@ferc.gov>; [REDACTED]  
[REDACTED]  
Subject: NP18-7 questions

We have some questions regarding the full NOP, NP18-7:

Redacted pursuant to FOIA Exemptions 3 and 7

### Risk Analysis

[REDACTED]

[REDACTED]

[REDACTED]

- The Stipulated Incident Facts state [REDACTED]
- [REDACTED]
- [REDACTED]

4/14/2018

Mail - Kal.Ayoub@ferc.gov

[REDACTED]

Mitigation of Risk

In the URE mitigation plan, the plan detail section states

[REDACTED]

- [REDACTED]

- [REDACTED]

The Stipulated Incident Facts state

[REDACTED] Domain  
Name (@pge.com),  
[REDACTED]

- [REDACTED]

- **If so, please describe and explain the analysis performed and the detailed results.**

- [REDACTED]

- [REDACTED]

- [REDACTED]

4/14/2018

Mail - Kal.Ayoub@ferc.gov

Please provide your response on or before April 16, 2018.

Thank you,

**Bob Chambers**  
**Manager – Security Group 1**  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-665-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. All information herein contains staff pre-decisional deliberations, privileged or confidential, commercial, or financial information, and/or critical energy infrastructure information and is not for public release. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and do not reflect those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.

KA

Doc. 5

**Kal Ayoub**

---

**From:** Robert Chambers  
**Sent:** Thursday, April 05, 2018 5:10 PM  
**To:** Cynthia Pointer  
**Cc:** Kal Ayoub  
**Subject:** FW: NP18-7 questions

FYI...

Redacted pursuant to FOIA Exemption 6

**From:** Robert Chambers  
**Sent:** Monday, April 02, 2018 7:43 AM  
**To:** 'Ed Kichline' <Ed.Kichline@nerc.net>; Leigh Anne Faugust <Leigh.Faugust@nerc.net>  
**Cc:** Loye Hull <loye.hull@ferc.gov>; Lea [REDACTED]  
**Subject:** RE: NP18-7 questions

Good morning Ed,

If that is possible in the future, we will let you know...

**Bob Chambers**  
**Manager – Security Group 1**  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-865-1608  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

**From:** Ed Kichline [<mailto:Ed.Kichline@nerc.net>]  
**Sent:** Friday, March 30, 2018 1:28 PM  
**To:** Robert Chambers <[Robert.Chambers@ferc.gov](mailto:Robert.Chambers@ferc.gov)>; Leigh Anne Faugust <[Leigh.Faugust@nerc.net](mailto:Leigh.Faugust@nerc.net)>  
**Cc:** Loye Hull <[Loye.Hull@ferc.gov](mailto:Loye.Hull@ferc.gov)>; [REDACTED]  
**Subject:** RE: NP18-7 questions

Bob,

We will send these questions to WECC to start working along with the registered entity on the responses.

Loye had indicated in early March that there might be questions on the Full NOP. If possible in future months, we would appreciate if you could let us know that it is likely the Commission will extend its period for review prior to issuance of the Commission's Notice. That can help us keep the Regional Entity, the registered entity, and our management informed and result in less alarm when there is a Notice of Further Review.

Thank you,

Ed



---

**Ed Kichline**

**Senior Counsel and Director of Enforcement Oversight**

North American Electric Reliability Corporation

1325 G Street NW, Suite 600

Washington, DC 20005

202-400-3025 office | 917-754-3202 cell

[ed.kichline@nerc.net](mailto:ed.kichline@nerc.net)

[Twitter @NERC\\_Official](#) | [LinkedIn](#)

**Reliability | Accountability**

This email and any attachments are confidential. They may contain legal, professional, proprietary and/or other privileged information. They also may contain information that is subject to copyright belonging to NERC. This email and any attachments are intended solely for the addressee(s). If you are not the intended recipient, do not use the information in this email in any way, permanently delete this email and any attachments and notify the sender immediately. Redacted pursuant to FOIA Exemption 6

---

**From:** Robert Chambers [<mailto:Robert.Chambers@ferc.gov>]

**Sent:** Friday, March 30, 2018 11:58 AM

**To:** Leigh Anne Faugust <[Leigh.Faugust@nerc.net](mailto:Leigh.Faugust@nerc.net)>

**Cc:** Ed Kichline <[Ed.Kichline@nerc.net](mailto:Ed.Kichline@nerc.net)>; Love Hull <[Love.Hull@ferc.gov](mailto:Love.Hull@ferc.gov)>; [REDACTED]

**Subject:** NP18-7 questions

We have some questions regarding the full NOP, NP18-7:

Redacted pursuant FOIA Exemptions 3 and 7

**Risk Analysis**

[REDACTED]

[REDACTED]

[REDACTED]

- **The Stipulated Incident Facts** [REDACTED]

[REDACTED]

[REDACTED]

**Mitigation of Risk**

In the URE mitigation plan, the plan detail section states

[REDACTED]

[REDACTED]

[REDACTED]

The Stipulated Incident Facts state

[REDACTED] *Domain*  
*Name (@pge.com),*  
[REDACTED]

[REDACTED]

- If so, please describe and explain the analysis performed and the detailed results.

- [REDACTED]

- [REDACTED]

•   
Please provide your response on or before April 16, 2018.

Thank you,

**Bob Chambers**  
**Manager – Security Group 1**  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-665-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. All information herein contains staff pre-decisional deliberations, privileged or confidential, commercial, or financial information, and/or critical energy infrastructure information and is not for public release. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and do not reflect those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.

Warning: This email comes from an external sender. Be cautious when opening URLs or attachments from external senders.

CP

Doc. 6

Redacted pursuant to FOIA Exemption 6

**From:** Robert Chambers  
**To:** David Ortiz; [redacted]; Hegerle; Olutayo Oyelade; [redacted];  
**Cc:** Loye Hull; [redacted]  
**Subject:** FW: NP18-7 questions  
**Date:** Friday, March 30, 2018 12:00:14 PM

---

FYI...

**From:** Robert Chambers  
**Sent:** Friday, March 30, 2018 11:58 AM  
**To:** 'Leigh Anne Faugust' <Leigh.Faugust@nerc.net>  
**Cc:** Ed Kichline (Ed.Kichline@nerc.net) <Ed.Kichline@nerc.net>; Loye Hull <loye.hull@ferc.gov>; [redacted]  
**Subject:** NP18-7 questions

We have some questions regarding the full NOP, NP18-7:

**Risk Analysis**

Redacted pursuant to FOIA Exemptions 3 and 7

[redacted]

- [redacted]

[redacted]

- **The Stipulated Incident Facts state** [redacted]

- [redacted]

- [redacted]

[REDACTED]

**Mitigation of Risk**

In the URE mitigation plan, the plan detail section states [REDACTED]  
[REDACTED]  
[REDACTED]

■ [REDACTED]  
[REDACTED]

■ [REDACTED]  
[REDACTED]

The Stipulated Incident Facts state [REDACTED]  
[REDACTED]  
[REDACTED]  
*Domain Name (@pge.com),*  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

■ [REDACTED]  
[REDACTED]  
[REDACTED]

- **If so, please describe and explain the analysis performed and the detailed results.**
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]

Please provide your response on or before April 16, 2018.

Thank you,

**Bob Chambers**  
**Manager – Security Group 1**  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-665-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. All information herein contains staff pre-decisional deliberations, privileged or confidential, commercial, or financial information, and/or critical energy infrastructure information and is not for public release. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and do not reflect those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.

RC

Doc. 7

Redacted pursuant to FOIA Exemption 6

**From:** Robert Chambers  
**To:** "Ed Kichline"; Leigh Anne Faugust  
**Cc:** Loye Hull; [REDACTED]  
**Subject:** RE: NP18-7 questions  
**Date:** Monday, April 02, 2018 7:42:00 AM

---

Good morning Ed,

If that is possible in the future, we will let you know...

**Bob Chambers**  
**Manager – Security Group 1**  
 Federal Energy Regulatory Commission  
 Office of Electric Reliability (OER)  
 Division of Reliability Standards and Security  
 301-665-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

**From:** Ed Kichline [mailto:Ed.Kichline@nerc.net]  
**Sent:** Friday, March 30, 2018 1:28 PM  
**To:** Robert Chambers <Robert.Chambers@ferc.gov>; Leigh Anne Faugust <Leigh.Faugust@nerc.net>  
**Cc:** [REDACTED]  
**Subject:** RE: NP18-7 questions

Bob,

We will send these questions to WECC to start working along with the registered entity on the responses.

Loye had indicated in early March that there might be questions on the Full NOP. If possible in future months, we would appreciate if you could let us know that it is likely the Commission will extend its period for review prior to issuance of the Commission's Notice. That can help us keep the Regional Entity, the registered entity, and our management informed and result in less alarm when there is a Notice of Further Review.

Thank you,

Ed

---

**Ed Kichline**  
**Senior Counsel and Director of Enforcement Oversight**  
 North American Electric Reliability Corporation  
 1325 G Street NW, Suite 600  
 Washington, DC 20005  
 202-400-3025 office | 917-754-3202 cell  
[ed.kichline@nerc.net](mailto:ed.kichline@nerc.net)

[Twitter @NERC\\_Official](#) | [LinkedIn](#)  
**Reliability | Accountability**

This email and any attachments are confidential. They may contain legal, professional, proprietary and/or other privileged information. They also may contain information that is subject to copyright belonging to NERC. This email and any attachments are intended solely for the addressee(s). If you are not the intended recipient, do not use the information in this email in any way, permanently delete this email and any attachments and notify the sender immediately.

Redacted pursuant to FOIA Exemption 6  
**From:** Robert Chambers [mailto:Robert.Chambers@ferc.gov]  
**Sent:** Friday, March 30, 2018 11:58 AM  
**To:** Leigh Anne Faugust <Leigh.Faugust@nerc.net>  
**Cc:** Ed Kichline <Ed.Kichline@nerc.net>; Loye Hull <Loye.Hull@ferc.gov>; [REDACTED]  
**Subject:** NP18-7 questions

Redacted pursuant to FOIA Exemptions 3 and 7

We have some questions regarding the full NOP, NP18-7:

**Risk Analysis**

[REDACTED]

- [REDACTED]

[REDACTED]

- **The Stipulated Incident Facts state** [REDACTED]

[REDACTED]

[REDACTED]



[Redacted]

**Mitigation of Risk**

In the URE mitigation plan, the plan detail section states [Redacted]

- [Redacted]

- [Redacted]

The Stipulated Incident Facts state [Redacted]

[Redacted]

[Redacted] *Domain Name (@pge.com)*, [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]

- If so, please describe and explain the analysis performed and the detailed results.

- [Redacted]

- [Redacted]

[Redacted]

Please provide your response on or before April 16, 2018.

Thank you,

**Bob Chambers**  
**Manager – Security Group 1**  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
Division of Reliability Standards and Security  
301-465-1606  
[robert.chambers@ferc.gov](mailto:robert.chambers@ferc.gov)

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. All information herein contains staff pre-decisional deliberations, privileged or confidential, commercial, or financial information, and/or critical energy infrastructure information and is not for public release. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and do not reflect those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.

Warning: This email comes from an external sender. Be cautious when opening URLs or attachments from external senders.

**Exhibit O**  
**To Petition for Rulemaking**  
**Submitted by Michael Mabee**

"Unidentified Registered Entity" Dockets 2010-2018

Date	FERC Docket Number	Region	Registered Entity	Entities	Total Penalty (\$)	NOP	Order	A2 Spreadsheet
7/6/2010	NP10-130-000	SERC	Unidentified Registered Entity	1	\$0	<a href="#">View NOP</a>	<a href="#">View Order</a>	
7/6/2010	NP10-131-000	SERC	Unidentified Registered Entity	1	\$5,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
7/6/2010	NP10-134-000	SPP	Unidentified Registered Entity	1	\$0	<a href="#">View NOP</a>	<a href="#">View Order</a>	
7/6/2010	NP10-135-000	WECC	Unidentified Registered Entity	1	\$8,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
7/6/2010	NP10-136-000	WECC	Unidentified Registered Entity	1	\$7,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
7/6/2010	NP10-137-000	WECC	Unidentified Registered Entity	1	\$39,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
7/6/2010	NP10-138-000	RFC	Unidentified Registered Entity	1	\$5,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
7/6/2010	NP10-139-000	WECC	Unidentified Registered Entity	1	\$3,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
7/6/2010	NP10-140-000	RFC	Unidentified Registered Entity	1	\$5,600	<a href="#">View NOP</a>	<a href="#">View Order</a>	<a href="#">View Data request</a>
7/30/2010	NP10-159-000	WECC	Unidentified Registered Entity	1	\$109,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
9/13/2010	NP10-160-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View NOP</a>	<a href="#">View Order 1</a>	<a href="#">NERC Filing</a>
10/7/2010	NP11-1-000	WECC	Unidentified Registered Entity	1	\$106,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
10/7/2010	NP11-2-000	WECC	Unidentified Registered Entity	1	\$9,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
10/7/2010	NP11-3-000	SERC	Unidentified Registered Entity	1	\$6,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	<a href="#">View Data Request</a>
10/7/2010	NP11-4-000	FRCC	Unidentified Registered Entity	1	\$250,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
10/7/2010	NP11-5-000	SERC	Unidentified Registered Entity	1	\$16,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	<a href="#">View Data Request</a>
11/5/2010	NP11-21-000	RFC	Unidentified Registered Entity	1	\$8,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
11/5/2010	NP11-22-000	SERC	Unidentified Registered Entity	1	\$5,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
11/30/2010	NP11-47-000	SERC	Unidentified Registered Entity	1	\$0	<a href="#">View NOP</a>	<a href="#">View Order</a>	
11/30/2010	NP11-56-000	SERC	Unidentified Registered Entity	1	\$0	<a href="#">View NOP</a>	<a href="#">View Order</a>	
12/22/2010	NP11-59-000	RFC	Unidentified Registered Entity	1	\$7,000	<a href="#">View NOP</a>	<a href="#">View Extension</a>	
12/22/2010	NP11-63-000	WECC	Unidentified Registered Entity	1	\$80,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
12/22/2010	NP11-64-000	WECC	Unidentified Registered Entity	1	\$38,500	<a href="#">View NOP</a>	<a href="#">View Order</a>	
12/22/2010	NP11-70-000	WECC	Unidentified Registered Entity	1	\$55,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
12/22/2010	NP11-72-000	SERC	Unidentified Registered Entity	1	\$2,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
12/22/2010	NP11-76-000	SERC	Unidentified Registered Entity	1	\$0	<a href="#">View NOP</a>	<a href="#">View Order</a>	
12/22/2010	NP11-79-000	FRCC	Unidentified Registered Entity	1	\$100,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
12/22/2010	NP11-81-000	MRO, SPP	Unidentified Registered Entities	2	\$50,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
1/31/2011	NP11-102-000	WECC	Unidentified Registered Entity	1	\$6,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
1/31/2011	NP11-98-000	WECC	Unidentified Registered Entity	1	\$5,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/1/2011	NP11-104-000	Various	<b>Unidentified Registered Entities</b>	6	\$9	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
2/23/2011	NP11-106-000	RFC	Unidentified Registered Entity	1	\$15,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/23/2011	NP11-111-000	MRO	Unidentified Registered Entity	1	\$120,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/23/2011	NP11-116-000	FRCC	Unidentified Registered Entity	1	\$75,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/23/2011	NP11-124-000	RFC	Unidentified Registered Entity	1	\$100,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/23/2011	NP11-125-000	SPP, RFC	Unidentified Registered Entity	1	\$77,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/23/2011	NP11-127-000	FRCC	Unidentified Registered Entity	1	\$55,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/23/2011	NP11-128-000	WECC	Unidentified Registered Entity	1	\$450,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/28/2011	NP11-133-000	Various	<b>Unidentified Registered Entities</b>	5	\$11,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
3/30/2011	NP11-136-000	WECC	Unidentified Registered Entity	1	\$14,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-137-000	WECC	Unidentified Registered Entity	1	\$106,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-140-000	WECC	Unidentified Registered Entity	1	\$27,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-143-000	SERC	Unidentified Registered Entity	1	\$5,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-145-000	WECC	Unidentified Registered Entity	1	\$13,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-146-000	RFC	Unidentified Registered Entities	3	\$52,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	

"Unidentified Registered Entity" Dockets 2010-2018

Date	FERC Docket Number	Region	Registered Entity	Entities	Total Penalty (\$)	NOP	Order	A2 Spreadsheet
3/30/2011	NP11-149-000	RFC	Unidentified Registered Entity	1	\$20,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-150-000	MRO	Unidentified Registered Entity	1	\$0	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-155-000	WECC	Unidentified Registered Entity	1	\$2,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-156-000	SERC	Unidentified Registered Entity	1	\$12,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-157-000	SERC	Unidentified Registered Entity	1	\$7,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2011	NP11-161-000	WECC	Unidentified Registered Entity	1	\$35,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/31/2011	NP11-162-000	TRE, NPCC	Unidentified Registered Entities	2	\$10,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
4/29/2011	NP11-166-000	SPP, TRE	Unidentified Registered Entity	1	\$50,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/29/2011	NP11-167-000	WECC	Unidentified Registered Entity	1	\$89,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/29/2011	NP11-174-000	RFC	Unidentified Registered Entity	1	\$15,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/29/2011	NP11-175-000	WECC	Unidentified Registered Entity	1	\$32,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/29/2011	NP11-176-000	WECC	Unidentified Registered Entity	1	\$80,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/29/2011	NP11-178-000	WECC	Unidentified Registered Entity	1	\$35,000	<a href="#">View NOP &gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/29/2011	NP11-179-000	MRO	Unidentified Registered Entity	1	\$10,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/29/2011	NP11-180-000	WECC	Unidentified Registered Entity	1	\$71,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/29/2011	NP11-181-000	FRCC, NPCC	Unidentified Registered Entities	6	\$39,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
5/26/2011	NP11-182-000	WECC	Unidentified Registered Entity	1	\$59,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
5/26/2011	NP11-184-000	RFC	Unidentified Registered Entity	1	\$70,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View Data Request &gt;&gt;</a>
5/26/2011	NP11-188-000	SPP	Unidentified Registered Entity	1	\$16,860	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
5/26/2011	NP11-189-000	FRCC	Unidentified Registered Entity	1	\$17,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
5/26/2011	NP11-192-000	WECC	Unidentified Registered Entity	1	\$12,200	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
5/26/2011	NP11-193-000	WECC	Unidentified Registered Entity	1	\$60,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
5/26/2011	NP11-198-000	SPP	Unidentified Registered Entity	1	\$17,860	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
5/26/2011	NP11-199-000	Various	Unidentified Registered Entities	3	\$3,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
6/29/2011	NP11-204-000	WECC	Unidentified Registered Entity	1	\$37,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
6/29/2011	NP11-205-000	WECC	Unidentified Registered Entity	1	\$22,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
6/29/2011	NP11-206-000	NPCC	Unidentified Registered Entity	3	\$80,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View Supplemental &gt;&gt;</a>
6/29/2011	NP11-211-000	WECC	Unidentified Registered Entity	1	\$14,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
6/29/2011	NP11-212-000	WECC	Unidentified Registered Entity	1	\$381,600	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
6/29/2011	NP11-213-000	WECC	Unidentified Registered Entity	1	\$143,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View Supplemental &gt;&gt;</a>
6/29/2011	NP11-218-000	WECC	Unidentified Registered Entity	1	\$130,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
6/29/2011	NP11-223-000	SPP	Unidentified Registered Entity	1	\$30,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
6/29/2011	NP11-225-000	RFC	Unidentified Registered Entity	1	\$10,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
6/29/2011	NP11-226-000	RFC	Unidentified Registered Entity	1	\$85,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-229-000	WECC	Unidentified Registered Entity	1	\$75,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-230-000	RFC	Unidentified Registered Entity	1	\$18,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-233-000	WECC	Unidentified Registered Entity	1	\$70,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-234-000	WECC	Unidentified Registered Entity	1	\$35,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-237-000	RFC	Unidentified Registered Entity	3	\$180,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-243-000	RFC	Unidentified Registered Entity	1	\$20,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-247-000	RFC	Unidentified Registered Entity	1	\$15,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-248-000	WECC	Unidentified Registered Entity	1	\$5,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-249-000	WECC	Unidentified Registered Entity	1	\$18,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-250-000	WECC	Unidentified Registered Entity	1	\$12,600	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/28/2011	NP11-251-000	WECC	Unidentified Registered Entity	1	\$7,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	

"Unidentified Registered Entity" Dockets 2010-2018

Date	FERC Docket Number	Region	Registered Entity	Entities	Total Penalty (\$)	NOP	Order	A2 Spreadsheet
7/29/2011	NP11-253-000	Various	Unidentified Registered Entities	8	\$26,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
8/31/2011	NP11-261-000	RFC	Unidentified Registered Entity	1	\$70,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
8/31/2011	NP11-262-000	SPP	Unidentified Registered Entity	1	\$12,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
8/31/2011	NP11-263-000	TRE	Unidentified Registered Entity	1	\$11,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
8/31/2011	NP11-264-000	SPP	Unidentified Registered Entity	1	\$8,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
8/31/2011	NP11-266-000	Various	Unidentified Registered Entities	5	\$63,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
9/30/2011	NP11-269-000	WECC	Unidentified Registered Entity	1	\$225,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
9/30/2011	NP11-270-000	Various	Unidentified Registered Entities	21	\$193,900	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
9/30/2011	RC11-6-000	Various	Unidentified Registered Entities	59	\$0	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-1 Spreadsheet &gt;&gt;</a>
10/31/2011	NP12-1-000	RFC	Unidentified Registered Entities	3	\$275,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Corrected Spreadsheet &gt;&gt;</a>
10/31/2011	NP12-2-000	Various	Unidentified Registered Entities	16	\$184,200	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
10/31/2011	RC12-1-000	Various	Unidentified Registered Entities	33	\$0	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-1 Spreadsheet &gt;&gt;</a>
11/30/2011	NP12-3-000	WECC	Unidentified Registered Entity	1	\$125,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
11/30/2011	NP12-4-000	WECC	Unidentified Registered Entity	1	\$160,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
11/30/2011	NP12-5-000	RF, WECC	Unidentified Registered Entities	12	\$89,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
11/30/2011	RC12-2-000	Various	Unidentified Registered Entities	30	\$0	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-1 Spreadsheet &gt;&gt;</a>
12/30/2011	NP12-10-000	Various	Unidentified Registered Entities	21	\$109,600	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Corrected Spreadsheet &gt;&gt;</a>
12/30/2011	NP12-9-000	RFC	Unidentified Registered Entity	1	\$60,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
12/30/2011	RC12-6-000	Various	Unidentified Registered Entities	40	\$0	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-1 Spreadsheet &gt;&gt;</a>
1/31/2012	NP12-11-000	WECC	Unidentified Registered Entity	1	\$135,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
1/31/2012	NP12-12-000	Various	Unidentified Registered Entities	18	\$160,500	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
1/31/2012	RC12-7-000	Various	Unidentified Registered Entities	30	\$0	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/29/2012	NP12-16-000	WECC	Unidentified Registered Entity	1	\$80,000	Filing		
2/29/2012	NP12-17-000	SPP RE	Unidentified Registered Entity	1	\$40,000	Filing		
2/29/2012	NP12-18-000	Various	Unidentified Registered Entities	23	\$222,900	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
2/29/2012	RC12-8-000	Various	Unidentified Registered Entities	24	\$0	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-1 Spreadsheet &gt;&gt;</a>
3/30/2012	NP12-20-000	WECC	Unidentified Registered Entity	1	\$60,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/30/2012	NP12-22-000	Various	Unidentified Registered Entities	15	\$42,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
3/30/2012	RC12-10-000	Various	Unidentified Registered Entities	12	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
4/30/2012	NP12-25-000	RFC	Unidentified Registered Entity	1	\$115,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/30/2012	NP12-26-000	Various	Unidentified Registered Entities	18	\$95,300	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
4/30/2012	RC12-11-000	Various	Unidentified Registered Entities	18	\$0	<a href="#">View Supplemental</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
5/30/2012	NP12-27-000	Various	Unidentified Registered Entities	20	\$48,600	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet</a>
5/30/2012	NP12-29-000	WECC	Unidentified Registered Entity	1	\$162,200	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
5/30/2012	RC12-12-000	Various	Unidentified Registered Entities	40	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
6/29/2012	NP12-36-000	Various	Unidentified Registered Entities	15	\$121,900	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet</a>
6/29/2012	RC12-13-000	Various	Unidentified Registered Entities	40	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
7/31/2012	NP12-37-000	WECC	Unidentified Registered Entities	4	\$134,350	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/31/2012	NP12-38-000	WECC	Unidentified Registered Entity	1	\$72,000	Filing	<a href="#">View Order &gt;&gt;</a>	
7/31/2012	NP12-40-000	Various	Unidentified Registered Entities	15	\$101,100	Filing	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
7/31/2012	RC12-14-000	Various	Unidentified Registered Entities	30	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
8/31/2012	NP12-43-000	WECC	Unidentified Registered Entity	1	\$70,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
8/31/2012	NP12-44-000	Various	Unidentified Registered Entities	16	\$182,800	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
8/31/2012	RC12-15-000	Various	Unidentified Registered Entities	38	\$0	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
9/28/2012	NP12-45-000	FRCC	Unidentified Registered Entity	1	\$150,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	

"Unidentified Registered Entity" Dockets 2010-2018

Date	FERC Docket Number	Region	Registered Entity	Entities	Total Penalty (\$)	NOP	Order	A2 Spreadsheet
9/28/2012	NP12-46-000	WECC	Unidentified Registered Entity	1	\$200,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
9/28/2012	NP12-47-000	Various	Unidentified Registered Entities	14	\$113,400	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
9/28/2012	RC12-16-000	Various	Unidentified Registered Entities	41	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
10/31/2012	NP13-1-000	WECC	Unidentified Registered Entity	1	\$200,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
10/31/2012	NP13-4-000	RFC	Unidentified Registered Entities	3	\$725,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
10/31/2012	NP13-5-000	Various	<b>Unidentified Registered Entities</b>	19	\$216,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
10/31/2012	RC13-1-000	Various	<b>Unidentified Registered Entities</b>	44	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
11/30/2012	NP13-6-000	WECC	Unidentified Registered Entity	1	\$62,500	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
11/30/2012	RC13-2-000	Various	<b>Unidentified Registered Entities</b>	25	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
12/31/2012	NP13-11-000	<b>SPP</b>	<b>Unidentified Registered Entity</b>	1	<b>\$107,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View NOP &gt;&gt;</a>	
12/31/2012	NP13-12-000	Various	Unidentified Registered Entities	21	\$214,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
12/31/2012	NP13-16-000	<b>WECC</b>	<b>Unidentified Registered Entity</b>	1	<b>\$207,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View NOP &gt;&gt;</a>	
12/31/2012	NP13-17-000	<b>RFC</b>	<b>Unidentified Registered Entities</b>	3	<b>\$80,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
12/31/2012	NP13-18-000	<b>SPP</b>	<b>Unidentified Registered Entity</b>	1	<b>\$153,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View NOP &gt;&gt;</a>	
12/31/2012	NP13-19-000	<b>SERC</b>	<b>Unidentified Registered Entity</b>	1	<b>\$950,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View NOP &gt;&gt;</a>	
12/31/2012	RC13-3-000	Various	<b>Unidentified Registered Entities</b>	25	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
1/31/2013	NP13-22-000	<b>WECC</b>	<b>Unidentified Registered Entity</b>	1	<b>\$115,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
1/31/2013	NP13-23-000	Various	Unidentified Registered Entities	22	\$73,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
1/31/2013	RC13-5-000	Various	Unidentified Registered Entities	22	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
2/28/2013	<b>NP13-24-000</b>	<b>WECC</b>	<b>Unidentified Registered Entity</b>	3	<b>\$151,500</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
2/28/2013	NP13-27-000	Various	Unidentified Registered Entities	14	\$53,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
2/28/2013	RC13-6-000	Various	Unidentified Registered Entities	27	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
3/27/2013	<b>NP13-30-000</b>	<b>RFC</b>	<b>Unidentified Registered Entity</b>	3	<b>\$120,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View Errata &gt;&gt;</a>
3/27/2013	NP13-28-000	Various	<b>Unidentified Registered Entity</b>	1	<b>\$90,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
3/27/2013	NP13-29-000	Various	Unidentified Registered Entities	10	\$80,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
4/30/2013	NP13-32-000	NERC	<b>Unidentified Registered Entity</b>	1	<b>\$40,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
4/30/2013	NP13-33-000	Various	Unidentified Registered Entities	18	\$315,250	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
4/30/2013	RC13-8-000	Various	Unidentified Registered Entities	50	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
5/30/2013	NP13-34-000	<b>Texas RE</b>	<b>Unidentified Registered Entity</b>	1	<b>\$137,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View Errata &gt;&gt;</a>
5/30/2013	NP13-38-000	<b>WECC</b>	<b>Unidentified Registered Entity</b>	1	<b>\$291,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
5/30/2013	NP13-39-000	Various	Unidentified Registered Entities	16	\$67,500	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
5/30/2013	RC13-9-000	Various	Unidentified Registered Entities	53	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
6/27/2013	NP13-41-000	Various	Unidentified Registered Entities	20	\$198,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
6/27/2013	RC13-10-000	Various	Unidentified Registered Entities	52	\$0	<a href="#">View Filing &gt;&gt;</a>		<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
7/31/2013	NP13-45-000	<b>WECC</b>	<b>Unidentified Registered Entity</b>	1	<b>\$198,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
7/31/2013	NP13-46-000	Various	Unidentified Registered Entities	18	\$112,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
7/31/2013	NP13-47-000	<b>RFC, SERC</b>	Unidentified Registered Entities	2	<b>\$350,000</b>	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
8/30/2013	NP13-51-000	Various	Unidentified Registered Entities	18	\$98,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
9/30/2013	NP13-55-000	WECC	Unidentified Registered Entity	1	\$150,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
9/30/2013	NP13-57-000	Various	Unidentified Registered Entities	12	\$189,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
10/30/2013	NP14-4-000	RF, SERC	Unidentified Registered Entities	16	\$55,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
10/30/2013	NP14-5-000	RFC	Unidentified Registered Entity	1	\$0	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	
11/27/2013	NP14-6-000	Various	Unidentified Registered Entities	14	\$142,000	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
12/30/2013	NP14-14-000	Various	Unidentified Registered Entities	18	\$276,500	<a href="#">View Filing &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	<a href="#">View A-2 Spreadsheet &gt;&gt;</a>
12/30/2013	NP14-16-000	SERC	Unidentified Registered Entity	1	\$50,000	<a href="#">View NOP &gt;&gt;</a>	<a href="#">View Order &gt;&gt;</a>	

"Unidentified Registered Entity" Dockets 2010-2018

Date	FERC Docket Number	Region	Registered Entity	Entities	Total Penalty (\$)	NOP	Order	A2 Spreadsheet
12/30/2013	NP14-17-000	WECC	Unidentified Registered Entity	1	\$144,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
12/30/2013	NP14-18-000	SERC	Unidentified Registered Entity	1	\$110,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
12/30/2013	NP14-19-000	WECC	Unidentified Registered Entity	1	\$185,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	<a href="#">View Errata&gt;&gt;</a>
12/30/2013	NP14-20-000	SERC	Unidentified Registered Entity	1	\$198,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
12/30/2013	NP14-22-000	WECC	Unidentified Registered Entity	1	\$150,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
12/31/2013	NP14-21-000	SERC	Unidentified Registered Entity	1	\$175,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
12/31/2013	NP14-23-000	SPP RE	Unidentified Registered Entity	1	\$100,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
12/31/2013	NP14-24-000	SERC	Unidentified Registered Entity	1	\$350,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
12/31/2013	NP14-25-000	SERC	Unidentified Registered Entity	1	\$250,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
12/31/2013	NP14-26-000	SERC	Unidentified Registered Entity	1	\$120,000	<a href="#">View NOP&gt;&gt;</a>	<a href="#">View Order&gt;&gt;</a>	
2014-01-30	NP14-29-000	WECC	Unidentified Registered Entity	1	\$109,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
2014-01-30	NP14-30-000	RFC	Unidentified Registered Entity	1	\$75,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
2014-02-27	NP14-32-000	SPP RE	Unidentified Registered Entity	1	\$0	<a href="#">View NOP</a>	<a href="#">View Order</a>	
2014-03-31	NP14-37-000	WECC	Unidentified Registered Entity	1	\$465,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
2014-04-30	NP14-39-000	WECC	Unidentified Registered Entity	1	\$155,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
2014-05-29	NP14-41-000	WECC	Unidentified Registered Entity	1	\$98,500	<a href="#">View NOP</a>	<a href="#">View Order</a>	
2014-05-29	NP14-42-000	SERC	Unidentified Registered Entity	1	\$250,000	<a href="#">View NOP</a>	<a href="#">View Order</a>	
2014-07-31	NP14-45-000	WECC	Unidentified Registered Entity	1	\$180,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-07-31	NP14-46-000	RFC	Unidentified Registered Entities	7	\$50,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-08-27	NP14-48-000	RFC/NPCC	Unidentified Registered Entities	3	\$625,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-10-30	NP15-5-000	SPP	Unidentified Registered Entity	1	\$45,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-10-30	NP15-6-000	TRE	Unidentified Registered Entity	1	\$106,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-11-25	NP15-10-000	WECC	Unidentified Registered Entity	1	\$150,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-11-25	NP15-11-000	RFC	Unidentified Registered Entity	1	\$75,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-11-25	NP15-9-000	MRO	Unidentified Registered Entity	1	\$150,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-12-30	NP15-13-000	RFC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-12-30	NP15-15-000	SERC	Unidentified Registered Entities	2	\$120,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-12-30	NP15-17-000	WECC	Unidentified Registered Entity	1	\$120,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2014-12-30	NP15-18-000	Multiple	Unidentified Registered Entities	10	\$124,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	<a href="#">View A-2 Spreadsheet</a>
2015-02-26	NP15-20-000	SERC	Unidentified Registered Entity	1	\$70,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2015-03-31	NP15-23-000	WECC	Unidentified Registered Entities	3	\$165,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	<a href="#">View A-2 Spreadsheet</a>
2015-04-30	NP15-24-000	RFC	Unidentified Registered Entity	1	\$150,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2015-04-30	NP15-26-000	RFC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2015-08-31	NP15-33-000	RFC	Unidentified Registered Entity	1	\$425,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2015-10-29	NP16-2-000	WECC	Unidentified Registered Entity	1	\$160,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2015-12-01	NP16-4-000	WECC	Unidentified Registered Entity	1	\$205,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2015-12-01	NP16-5-000	WECC	Unidentified Registered Entity	1	\$200,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2015-12-30	NP16-7-000	SPP	Unidentified Registered Entity	1	\$235,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-01-28	NP16-10-000	RF	Unidentified Registered Entity	1	\$150,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-01-28	NP16-9-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-02-29	NP16-12-000	RF	Unidentified Registered Entity	1	\$1,700,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-04-28	NP16-18-000	RF / SERC	Unidentified Registered Entities	5	\$115,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	<a href="#">View A-2 Spreadsheet</a>
2016-05-31	NP16-20-000	FRCC	Unidentified Registered Entity	1	\$35,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	<a href="#">View A-2 Spreadsheet</a>
2016-07-28	NP16-23-000	SERC	Unidentified Registered Entity	1	\$225,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-07-28	NP16-24-000	SERC	Unidentified Registered Entity	1	\$180,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	



"Unidentified Registered Entity" Dockets 2010-2018

Date	FERC Docket Number	Region	Registered Entity	Entities	Total Penalty (\$)	NOP	Order	A2 Spreadsheet
2016-10-31	NP17-2-000	WECC	Unidentified Registered Entity	1	\$1,125,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-10-31	NP17-3-000	WECC	Unidentified Registered Entity	1	\$250,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-11-30	NP17-8-000	MRO	Unidentified Registered Entity	1	\$142,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-12-29	NP17-10-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-12-29	NP17-11-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Order</a>	
2016-12-29	NP17-12-000	WECC /SERC	Unidentified Registered Entities	4	\$60,000	<a href="#">View Filing</a>	<a href="#">View Order</a>	<a href="#">View A-2 Spreadsheet</a>
2016-12-29	NP17-13-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Notice</a>	
2017-04-27	NP17-21-000	WECC	Unidentified Registered Entity	1	\$201,000	<a href="#">View Filing</a>	<a href="#">View Notice</a>	
2017-07-31	NP17-25-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Notice</a>	<a href="#">View A-2</a>
2017-07-31	NP17-26-000	SPP RE	Unidentified Registered Entity	1	\$250,000	<a href="#">View Filing</a>	<a href="#">View Notice</a>	
2017-09-28	NP17-31-000	SERC	Unidentified Registered Entity	1	\$500,000	<a href="#">View Filing</a>	<a href="#">View Notice</a>	
2017-10-31	NP18-2-000	WECC	Unidentified Registered Entities	2	\$0	<a href="#">View Filing</a>	<a href="#">View Notice</a>	<a href="#">View A-2</a>
2018-02-28	NP18-7-000	WECC	Unidentified Registered Entity	1	\$2,700,000	<a href="#">View Filing</a>	<a href="#">View Notice</a>	
2018-05-31	NP18-14-000	RF	Unidentified Registered Entity	1	\$180,000	<a href="#">View Filing</a>	<a href="#">View Notice</a>	
2018-05-31	NP18-15-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Notice</a>	<a href="#">View A-2</a>
2018-07-31	NP18-21-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Notice</a>	<a href="#">View A-2</a>
2018-08-30	NP18-22-000	WECC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Notice</a>	
2018-09-27	NP18-26-000	NPCC	Unidentified Registered Entity	1	\$0	<a href="#">View Filing</a>	<a href="#">View Notice</a>	<a href="#">View A-2</a>