Michael Mabee
[redacted]
(516) 808-0883
Email: CivilDefenseBook@gmail.com
Web: https://michaelmabee.info/

December 1, 2019

New Hampshire Public Utilities Commission
21 S. Fruit St, Suite 10
Concord, N.H. 03301-2429

Via Email: Kate.Bailey@puc.nh.gov; Michael.Giaimo@puc.nh.gov; Dianne.Martin@puc.nh.gov

Dear Commissioners,

I wish to bring to your attention an issue of great importance to the citizens of New Hampshire and that should be of great interest to the Commission. The issue is that the North American Electric Reliability Corporation (NERC) has been withholding the names of regulatory violators submitted to the Federal Energy Regulatory Commission (FERC). Since July of 2010, the names of *every single company* that has violated of Critical Infrastructure protection (CIP) standards, which include cybersecurity and physical security standards, have been covered up from public view.

These unnamed violators almost certainly include companies regulated by the New Hampshire Public Utilities Commission. Unfortunately, FERC has delayed and denied the release of this information under the Freedom of Information Act.

There are several key reasons that the names of the regulatory violators are critical to the public and the Commission:

1. The public has a right to know if the company they are paying (and depending upon) for reliable electricity is a violator – or serial violator – of mandatory reliability standards.
2. The Commission needs to know about regulatory violations of mandatory reliability standards in order to make decisions on investments for mitigation, infrastructure improvement and for other regulatory purposes.
3. Presently, the regulatory violator decides whether the ratepayers or the shareholders eat the costs of the regulatory fines and mitigation costs related to the violations.

On the last point, it is very disturbing that absent transparency, the regulatory violator decides who pays. This is why it is critical that the FERC release the names of the regulatory violators along with sufficient information so that the public ("ratepayers"), investors ("shareholders"), the PUCs (the ones who should be making these decisions) and Congress (the oversight) can see what is happening.

The FERC Docket where this issue of transparency is being discussed is FERC Docket No. AD19-18-000. The comment period closed on October 28, 2019, however there is a pending motion for a public

hearing which was filed by the New Hampshire based Foundation for Resilient Societies, attached hereto as Appendix A. I am also attaching the comments of the New Mexico Public Regulation Commission (PRC) as Appendix B and the comments of the New Hampshire Office of Consumer Advocate as Appendix C. Finally, I am attaching my letter to the National Association of Regulatory Utility Commissioners (NARUC) as Appendix D. These filings should provide you with sufficient background.

The regulatory structure of the "electric grid" is mind-numbingly complex: there are more than 60 state and federal government regulators plus the nonprofit NERC and its seven Regional Entities. The FERC view of what constitutes the "electric grid" is likely limited to the "Bulk Power System" (BPS), however the public and the national security view includes all aspects of generation, transmission and distribution of electric power. Entities often overlap into generation, transmission and distribution; thus, many entities have multiple regulators at the state and federal level. The security needs of the entire system must be the focus, which underscores the mandate for transparency surrounding security violators anywhere in that system.

I request that the New Hampshire Public Utilities Commission file a request in this docket that FERC hold a public hearing (or Technical Conference). It is critical that the public utility commissions be heard on this issue.

Thank you for your attention to this critical matter,

Michael Mabee

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards	**)**	**Docket No. AD19-18-000**

Motion for the Commission to Hold a Public Hearing

Submitted to FERC on October 23, 2019

Pursuant to Rule 212 of the Federal Energy Regulatory Commission's ("Commission") Rules of Practice and Procedure,[1] the Foundation for Resilient Societies ("Resilient Societies"), hereby respectfully submits this motion for the Commission to hold a public hearing (or technical conference) on the facts and circumstances behind the ongoing concealment of the identities of utilities who violate electric reliability standards and additionally moves that Docket No. AD19-18-000 (or other docket established for the purpose of a hearing) remain open for public comment for 30 days after the date of the hearing.

This motion follows a recent circumstance where Pacific Gas & Electric (PG&E), a repeat reliability standards violator whose identity has been redacted in FERC dockets and who recently shut off power to 2 million California residents, has informed California Governor Gavin Newsom that the utility is expected to periodically and selectively shut off power for the next ten years to prevent wildfires. Moreover, PG&E also stated that it could shut off the company's entire electric grid at times — potentially affecting 5.4 million homes and businesses.[2]

[1] 18 C.F. R. § 385.212 (2018).
[2] Dale Kasler, Michael McGough, and Sophia Bollag,"PG&E will try to reduce blackout impact. It also says entire grid could go dark," *Sacramento Bee*, October 18, 2019.
https://www.sacbee.com/news/california/fires/article236411443.html

On information and belief, there are other utilities in the Bulk Power System who have likewise violated electric reliability standards, have pervasive management shortfalls, and whose identity has been concealed after standards violations. These violating utilities could cause economic losses and blackouts for ratepayers in their states and regions. Public utility commissions and ratepayers throughout the United States deserve a public hearing on the critical issue of transparency in enforcement of reliability standards.

BACKGROUND

On August 27, 2019, FERC opened Docket No. AD19-18-000 and requested comments on a Joint White Paper of the Commission and the North American Electric Reliability Corporation (NERC). The Joint White Paper proposed a change to the procedures for drafting NERC Notices of Penalty for violators of electric reliability standards, including disclosure of the identity of standards violators.

On September 19, 2019, in response to a motion by the Edison Electric Institute and other Trade Associations, the Commission granted an extension of time to comment until October 28, 2019.

On October 9, 2019, PG&E, a violator of vegetation management and CIP standards whose identity had been concealed, executed a Public Safety Power Shutdown for 600,000 ratepayers and an estimated 2 million California residents because high winds might cause vegetation to touch transmission lines, sparking wildfires. On October 18, 2019, PG&E informed the California Public Utilities Commission that the company's entire electric grid might be shut down in some future circumstances and that it could take a decade to remedy grid management deficiencies.[2]

On July 31, 2009, PG&E was fined $100,000 for violations of NERC Standard FAC-003-1 — Transmission Vegetation Management Program and other reliability standards.[3] It is not known if PG&E was subsequently citied for violations of NERC vegetation management standards because NERC began concealing the identities of standard violators in July 2010 for Notices of Penalty where violations of CIP standards also were found in the audit.[4]

On February 28, 2018, PG&E was fined $2.7 million for violations of CIP standards; on October 31, 2016, PG&E was fined $1.125 million for violations of CIP standards; on May 29, 2014, PG&E was fined $98,500 for violations of CIP standards. The Notices of Penalty (NOP) filed in the FERC Dockets redacted the identity of the violator in each of these cases—the PG&E's identity only became known through a Freedom of Information Act request filed by Michael Mabee, a private citizen, and reporting of the Wall Street Journal.[5] [6]

MOTION FOR A PUBLIC HEARING

Due to the long-term concealment of its identity as a standards violator, PG&E has escaped scrutiny by its state public utility commission and the ratepaying public. Deficient management practices at PG&E have not been previously remedied and now California ratepayers are faced with years of prospective blackouts from vegetation management shortfalls and possibly cybersecurity gaps as well. The same basic scenario has been observed

[3] FERC Docket NP09-35-000.
[4] Starting in July 2010, for standard violations that are part of a Notice of Penalty that containing CIP violations, NERC has designated the Registered Entity as "Unidentified Registered Entity," "Unidentified Registered Entities," or "NERC." See NERC Enforcement and Mitigation webpage, hyperlink for "Searchable NOP Spreadsheet," https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx. Accessed October 23, 2019.
[5] Rebecca Smith, "PG&E Among Utilities Cited for Failing to Protect Against Cyber and Physical Attacks," *Wall Street Journal*, April 9, 2019. https://www.wsj.com/articles/pg-e-among-utilities-cited-for-failing-to-protect-against-cyber-and-physical-attacks-11554821337
[6] FERC Dockets NP14-41-000, NP17-2-000, and NP18-7-000.

elsewhere for utilities under FERC jurisdiction. For example, on January 25, 2019, Duke Energy was fined $10 million for violations of CIP standards, but its identity was concealed until reporting by the Wall Street Journal.[7] [8]

On information and belief, utilities in other states and regions have violated electric reliability standards, but their identity has been concealed from their public utility commissions and the ratepaying public in the majority of instances, resulting in blackout risks and possibly ratepayer overcharges. According to the September 26, 2019 NERC Searchable NOP Spreadsheet, there were 6,317 standard violations filed from July 2010 to September 2019. For 3,892 of these violations, the identity of the utility was concealed.[9] The compliance enforcement system for reliability standards is vast, largely secret, and often unaccountable to public utility commissions and the ratepaying public.

For much of electric grid infrastructure, it is the public utility commissions that control cost recovery for grid reliability and security improvements. With information on standard violations routinely redacted in NERC Notices of Penalty and therefore withheld from state public utility commissions, the commissions lack factual record to approve cost recovery for hardware mitigations. In cases where standard violations are procedural in nature, the utilities may attempt to charge ratepayers for the monetary penalties without the knowledge of their public utility commission.

---

[7] Rebecca Smith, "Duke Energy Broke Rules Designed to Keep Electric Grid Safe," Wall Street Journal, February 1, 2019. https://www.wsj.com/articles/duke-energy-broke-rules-designed-to-keep-electric-grid-safe-11549056238

[8] FERC DocketNP19-4-000.

[9] Statistics based on searches of NERC Enforcement and Mitigation webpage, "Searchable NOP Spreadsheet," https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx. Accessed October 23, 2019.

A public hearing should examine the rationale for concealment of the identity of utilities who violate reliability standards. Such a hearing could call as witnesses the commissioners of state public utility commissions, as well as members of the ratepaying public who have been harmed or could be harmed, by higher rates and blackouts. Cybersecurity experts could testify on best practices for timely disclosure of vulnerabilities as established by the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security and the divergent practice of indefinite concealment by the electric utility industry and its regulatory apparatus.[10] In this matter involving both economic losses and potential deaths from blackout, docket comments are no substitute for in-person testimony before the Commission.

NOTICE AND COMMUNICATIONS

All notices and communications with respect to this proceeding should be directed to the representative listed below:

Thomas S. Popik
President
Foundation for Resilient Societies
24 Front Street, Suite 203
Exeter, NH 03833
(855) 688-2430 ext. 701
thomasp@resilientsocieties.org

[10] CISA has established seven-point criteria for release of cybersecurity vulnerabilities. See "CISA Vulnerability Disclosure Policy" at https://www.us-cert.gov/vulnerability-disclosure-policy.

CONCLUSION

WHEREFORE, for the foregoing reasons, Resilient Societies respectfully requests that the Commission grant this motion to conduct a hearing on the concealment of the identities of electric reliability standards violators and changes to the Commission's procedures that would remedy this.

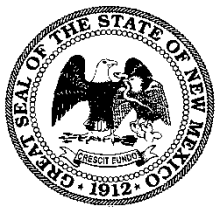
Respectfully submitted by:

Thomas S. Popik, President
thomasp@resilientsocieties.org

William R. Harris, Director and General Counsel
williamh@resilientsocieties.org

for the
Foundation for Resilient Societies
24 Front Street, Suite 203
Exeter, NH 03833
www.resilientsocieties.org

NEW MEXICO PUBLIC REGULATION COMMISSION



P.O. Box 1269
1120 Paseo de Peralta
Santa Fe, NM 87504-1269

Mr. Jonathan First
Office of the General Counsel
Federal Energy Regulatory Commission
888 First St., NE
Washington DC, 20426

November 27, 2019

Via E-File

Re: Proposed Revisions to the Federal Energy Regulatory Commission's *Notice of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards,* Docket AD No. 19-18-000

Dear Mr. First,

The New Mexico Public Regulation Commission (PRC) urges the Federal Energy Regulatory Commission (FERC) to strike the proper balance between legitimate cyber- and other security interests and the principles of openness and public accountability that are cornerstones of self-governance and democracy.[1] As a preliminary matter the PRC appreciates the changes made in the *Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards* (FERC/NERC, Docket No. 19-18-000, August 27, 2019)(*White Paper*); *viz.*, a cover letter disclosing the "name of the violator, the reliability standard(s) violated […] and the penalty amount".[2] The PRC supports the changes proposed to advance transparency, but urges even more openness to best serve the public interest.

The PRC is an independently elected commission that regulates three investor owned electric utilities, aspects of 16 rural electrical cooperatives and various other industries as directed by the state legislature. While our primary focus is on balancing the interests of rate payers and

[1] These principles are statutorily encoded in the Freedom of Information Act (5 USC §552) and New Mexico's Inspection of Public Records Act (NMSA 1978, §§ 14-2-1 et seq.).
[2] *White Paper* at 3.

regulated entities, we occasionally participate in Federal regulatory actions. We recognize that decisions made at the national and regional level can have enormous impact on New Mexico and we appreciate the opportunity to be heard on this vital issue.

FERC's concerns with security of the United States' grid system are well-taken, and grid security is a multi-faceted topic. Without minimizing the danger of cyber-attacks, perhaps of more pressing concern to the average New Mexican are forest fires. Since 2009, well over 2 million acres have burned in New Mexico and New Mexicans have been forced to evacuate their homes.[3] In fact, some of these fires have been caused by electric transmission and distribution infrastructure failures due to high winds. Additionally, cooperation and coordination of fire prevention and response is difficult in New Mexico because the State of New Mexico has a patchwork of federal, state and private land and critical infrastructure ownership. These unique factors in our State make free and open information about critical infrastructure an essential perquisite to preventing, mitigating and extinguishing forest fires in this drought prone, heavily forested state.

The PRC believes that two principles should guide the FERC's decision-making concerning the degree of openness in Notices of Penalty (NOP) for violations of Critical Infrastructure Protection (CIP).

1. The public has a right to know if any utility is not complying with FERC reliability standards and its wildfire prevention plans, as do local and statewide government agencies. This information could be useful to them in myriad ways, not the least of which is mitigation of forest fires.

2. Grid resiliency should be a primary value. To the extent keeping CIP outage information confidential undermines grid resiliency, the rules should be changed to promote more openness.

In consideration of these principles, the PRC therefore endorses the proposal of the New Hampshire Office of Consumer Advocate when it calls for even more transparency. In addition to what FERC/NERC have proposed in their *White Paper*, we agree that seven additional pieces of information should also be included in the Notice of Penalty.[4]

1. All information fields contained in the present searchable NOP spreadsheet used by NERC, including the name of the entity that committed the violation,

2. The date on which the violation was discovered,

3. The duration of the violation,

4. The manner in which the violation was discovered,

[3] http://www.emnrd.state.nm.us/SFD/FireMgt/Historical.html

[4] *Comments of the New Hampshire Office of Consumer Advocate* at 5-6, (Docket No. 19-18-000) (filed October 25, 2019)("NHOCA") quoting *Comments and Alternate Proposal of Michael Mabee* at 5-11.

5. A description of the violation in plain English,

6. Aggravating and mitigating factors bearing on the penalty assessment,

7. Any settlement agreement applicable to the NOP.[5]

With these additions, the PRC believes a more realistic and beneficial balance for the public interest is achieved. Thank you.

NEW MEXICO PUBLIC REGULATION COMMISSION

/s/ Stephen Fischmann, Electronically Signed
Stephen Fischmann
Designee on behalf of New Mexico Public Regulation Commission
Commissioner of District 5
P.O. Box 1269
Santa Fe, NM 87504
stephen.fischmann@state.nm.us

CC'd via e-mail:

Theresa Becenti-Aguilar, Chair, Commissioner of District 4; t.becenti@state.nm.us
Valerie Espinoza, Vice-Chair, Commissioner of District 3; valerie.espinoza@state.nm.us
Cynthia B. Hall, Commissioner of District 1; cynthia.hall@state.nm.us
Jefferson L. Byrd, Commissioner of District 2; jeff.byrd@state.nm.us

[5] NHOCA Comments at 5-6.

Document Content(s)

UNITED STATES OF AMERICA

BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards	))))	Docket No. AD19-18-000

COMMENTS OF THE
NEW HAMPSHIRE OFFICE OF THE CONSUMER ADVOCATE

The New Hampshire Office of the Consumer Advocate (NH OCA) hereby submits the following comments in response to the August 27, 2019 Notice seeking responses to the document entitled "Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards" (Staff White Paper) as issued by the FERC Staff in conjunction with the Staff of the North American Electric Reliability Corporation (NERC). For the reasons that follow, the NH OCA respectfully urges the FERC to embrace the premise of the Staff White Paper – that applicable law and public policy require more transparency when it comes to violations of critical infrastructure reliability standards – while going beyond the relatively modest reforms the White Paper actually proposes.

I. About the New Hampshire Office of the Consumer Advocate

Pursuant to N.H. RSA 363:28, II, the NH OCA is tasked with representing the interests of the Granite State's residential utility customers "in any proceeding

concerning rates, charges, tariffs, and consumer services before any board, commission, agency, court, or regulatory body in which the interests of residential utility customers are involved." Although retail rate cases and other matters within the jurisdiction of the New Hampshire Public Utilities Commission are the bread and butter of the NH OCA's work, we regularly participate in FERC proceedings. In addition, the NH OCA is an end-user member of NEPOOL, the official stakeholder advisory forum of the regional transmission organization ISO New England, which operates the bulk power transmission system and wholesale electricity markets of the six New England states.

Our involvement in regional and national matters is premised on the notion that many if not most key decisions, concerning not just rates but also the safety, reliability, flexibility and technological capabilities of electric service provided to consumers in New Hampshire, are made at the regional and federal levels. Additionally, we are an active participant in the investigative docket the New Hampshire Public Utilities Commission opened in 2015 on the subject of grid modernization (N.H. PUC Docket No. IR 15-296). Progress in that docket has been slow to achieve, and it has become apparent that concerns about cybersecurity are the principal reason New Hampshire has yet to adopt a new roadmap for grid modernization and electric distribution planning generally. We thus believe that it is important for our office to participate actively when matters related to cybersecurity and the protection of critical infrastructure come before regulators and other decisionmakers.

II. Appropriately calibrated transparency is a key element of cybersecurity.

As noted in the Staff White Paper, the issue under examination in this docket is a straightforward one: How transparent should the FERC be when it receives a Notice of Penalty (NOP) from NERC in its capacity as the FERC-certified electric reliability organization pursuant to section 215(c) of the Federal Power Act, 16 U.S.C. § 824o(c)? The Federal Power Act authorizes NERC to impose a penalty on a user, owner, or operator of the FERC-jurisdictional bulk power system, subject to review by the FERC upon receipt of the NOP and a timely request from the alleged violator. *See* Staff White Paper at 5. Specifically at issue here are alleged violation of reliability standards related to critical infrastructure protection (CIP) – i.e., cybersecurity. *Id.* at 2.

According to the Staff White Paper, the FERC's rules require the agency to treat as confidential anything contained in such NOPs based on the mere assertion by NERC that the information is CEII – i.e., critical energy/electric infrastructure information – "until such time as Commission staff finds that the information is not entitled to such treatment." *Id.* (citations omitted). Before 2018, this had the effect of shielding from public scrutiny essentially everything about cybersecurity violations described in NOPs, even the identity of the violators. *Id.* at 3. Then came the first of what proved to be a blizzard of requests for disclosure pursuant to the Freedom of Information Act. *Id.* This, in turn, led to the disclosure of the identity of violators "in some limited cases where the Commission staff has determined that

the release will not jeopardize the security of the Bulk-Power System if publicly disclosed." *Id.*

As one of her final acts a member of the FERC, Commissioner Cheryl LaFleur expressed concern about the "growing controversy" over the transparency of CIP-related NOPs and observed that "state regulators, members of the public, and others have a legitimate interest in such violations" such that the agency "should seek to achieve as much transparency as [it] can consistent with protecting legitimate security interests." Statement of Commissioner LaFleur (Aug. 27, 2019). Nevertheless, the Staff White Paper does not propose any revisions to the applicable FERC rules. It merely suggests an informal update of the format NERC uses to submit NOPs, so that such notices "would consist of a proposed public cover letter that discloses the name of the violator, the Reliability Standard(s) violated . . . and the penalty amount." Staff White Paper at 3; *see also id.* at 10 (clarifying that the disclosure of which Reliability Standard or Standards had been violated would not include disclosure of "the requirement or sub-requirement violated").

The reforms proposed in the Staff White Paper are necessary but not sufficient if the Commission is to achieve the goal described by former Commissioner LaFleur of achieving an appropriate balance between legitimate cybersecurity interests and the principles of openness and public accountability enshrined in the Freedom of Information Act. The need for transparency is all the more acute in these particular circumstances; via Section 215(c) of the Federal Power Act and the FERC's designation of an industry-sponsored organization

(NERC) as the nation's primary reliability watchdog, the federal government has substantially privatized an essential public function subject to carefully circumscribed oversight from the FERC. Thus, the remainder of these comments explain why the Commission should go beyond the recommendations contained in the Staff White Paper.

III. The Commission should adopt the Mabee alternative proposal.

The NH OCA urges the Commission to adopt the approach outlined in the September 3, 2019 pleading entitled "Comments and Alternate Proposal" and submitted by Michael Mabee of Mont Vernon, New Hampshire. As Mr. Mabee noted, the proposal contained in the Staff White Paper does not provide for the public disclosure of enough information "to allow for public, investor, Congressional and state scrutiny and evaluation of the violators and the regulatory system." Mabee Comments and Alternate Proposal at 5; *see also* September 26, 2019 letter from Reporters Committee for Freedom of the Press at 2 ("Meaningful oversight, accountability, and reform are predicated on the ability of the press and public to examine and scrutinize government records"). Mr. Mabee proposes that the FERC go beyond the mere disclosure of names, standards violated, and the penalties imposed and instead make publicly available these seven specific items:

- All information fields contained in the present Searchable NOP Spreadsheet used by NERC, including the name of the entity that committed the violation,
- The date on which the violation was discovered,
- The duration of the violation,

- The manner in which the violation was discovered,
- A description of the violation in plain English,
- Aggravating and mitigating factors bearing on the penalty assessment, and
- Any settlement agreement applicable to the NOP.

Mabee Comments and Alternate Proposal at 5. Mr. Mabee lays out in persuasive fashion the specific reasons why the disclosure of this specific constellation of information aids the cause of accountability. *See id.* at 5-11 (referring, *inter alia*, to regional violation patterns, the meaningful use of relational databases, evaluation of the effectiveness of the enforcement regime, statistical analysis, etc.). He notes that merely disclosing the reliability standard that was violated, without revealing the requirement or sub-requirement violated, is to provide information at such a level of bland generality as to be meaningless for purposes of public scrutiny. *Id.* at 7-9. He notes that these disclosures provide would-be cyber-no-goodniks no actionable information – and that, should there be any legitimate concerns to the contrary in any specific case, NERC can and should make a showing to that effect which would allow the FERC to redact information on a case-by-case basis. This is a very sound approach because it places the presumption where it belongs – in *favor* of disclosure.

Our experience, as a frequent litigant before the New Hampshire Public Utilities Commission and as an end-user member of NEPOOL (the stakeholder advisory board to the regional transmission organization ISO New England) is that electric utilities (i.e., the same firms that own the bulk power transmission system)

consistently rely on conclusory and self-serving allegations about the ill-effects of transparency to thwart efforts to hold them and their regulators publicly accountable. We see it at the state level when utilities claim, without proof, that they would suffer competitive harm by certain disclosures even though they are regulated monopolies. We see it at the regional level when industry insiders claim that opening their deliberations as RTO stakeholders would have a chilling effect on their discussions. *See, e.g., RTO Insider LLC v. New England Power Pool Participants Committee*, 167 FERC ¶ 61021 (2019) (concurring statement of Commissioner Glick) ("To paraphrase Justice Louis Brandeis, sunlight is the best disinfectant and it is hard for me to understand how barring public and press scrutiny will further NEPOOL's mission or, ultimately, its legitimacy as the forum for considering how ISO New England's actions affect its stakeholders").[1] And we see it here.

We do not begrudge utilities the opportunity to make these assertions, nor do we necessarily contend that all or even most such claims of harm or potential harm are meritless. Our point is merely to caution the FERC not to rely on such positions when unsupported by evidence or even arguments that go beyond tautologies. From the ratepayer perspective, such caution is especially warranted when the subject is cybersecurity. Cyber-threats have emerged as the excuse of the century for billions

[1] Commissioner Glick also observed: "Rather than trying to hide their discussions from the public, NEPOOL and its members would be better served by permitting public and press attendance, so that all entities—including those that cannot spend the time or money needed to attend all NEPOOL meetings—can remain informed of the discussions regarding the important issues under NEPOOL's purview. That result would lead to a more robust discussion of the issues and, ultimately, to better public policy."

and billions of dollars in new utility investments in circumstances that conveniently evade the traditional public scrutiny for prudence, used-and-usefulness, etc. In New Hampshire, the pending "grid modernization" investigation at the NH PUC is rife with claims by utilities that they should be allowed to make massive investments in cybersecurity defenses subject to automatic cost recovery whose scrutiny will occur, if at all, behind closed doors. *See* New Hampshire Public Utilities Commission, *Staff Recommendation on Grid Modernization* (Jan. 31, 2019) at 75 (calling for utility submission of integrated distribution plans for regulatory approval that do "not contain specific measures that may compromise the utility's security plan" but describe only a "high level approach in addressing cyber security and privacy in the various layers of the utility's system").[2] But we are reliably told by the utilities with which we have frequent contact that their systems are queried by potential cybercriminals repeatedly throughout every day. In these circumstances, it is simply not tenable for the FERC to conclude that the modest disclosures suggested by Mr. Mabee would give sophisticated cyber-criminals actionable information they do not already have.

IV. Conclusion

The Staff White Paper referenced four issues deemed relevant to the decision at hand: (1) potential security benefits, (2) potential security concerns, (3) implementation difficulties, and (4) "whether the proposed format provide[s]

[2] The referenced document was filed in New Hampshire PUC Docket No. IR 15-296 and is available at https://www.puc.nh.gov/Regulatory/Docketbk/2015/15-296/LETTERS-MEMOS-TARIFFS/15-296_2019-02-12_STAFF_REPORT_AND_RECOMMENDATION.PDF.

sufficient transparency to the public." Staff White Paper at 4. For the reasons described above, the proposal contained in the Staff White Paper is laudable but ultimately inadequate to the needs of transparency and accountability. We respectfully request that the FERC put commenters with different perspectives to their proof by requiring them to come forward with persuasive evidence of security concerns implicated by the proposals in the Staff White Paper and Mr. Mabee's comments. Please do not let entrenched industry insiders use cybersecurity scare tactics to justify shielding them from public accountability.

Respectfully submitted,

D. Maurice Kreis
Consumer Advocate

Office of the Consumer Advocate
21 South Fruit Street, Suite 18
Concord, New Hampshire 03301
603.271.1174 (direct line)
donald.kreis@oca.nh.gov

October 25, 2019

Document Content(s)

Michael Mabee
[redacted]
(516) 808-0883
CivilDefenseBook@gmail.com
www.MichaelMabee.info

October 26, 2019

National Association of Regulatory Utility Commissioners
1101 Vermont Avenue, NW
Suite 200
Washington, DC 20005

Dear NARUC,

I am a citizen who conducts public interest research on the security of the electric grid. I have conducted several recent studies which raise significant regulatory red flags. I write to you gravely concerned that the public – and Congress – are receiving inadequate and misleading information about physical security and cybersecurity threats to the electric grid. It is my hope that this information will be helpful to engage the Public Utility Commissions to demand better information from the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC) and the Department of Energy (DOE).

As detailed in the attached report of my research, which I filed with FERC on October 25, 2019, I have uncovered the following:

1. Vast Disparities Exist in Electric Grid Incident Reporting Among Official Sources.

- *Physical Attacks:* There were 578 physical attacks against the grid reported to the Department of Energy from January 1, 2010 through May 31, 2019. Yet according the NERC annual reliability reports, there was only one during the same period.

- *Cyber Attacks:* There were 29 cyberattacks against the grid reported to the Department of Energy (DOE) from January 1, 2010 through May 31, 2019. The Department of Homeland Security (DHS) reports substantially higher numbers of attacks per year than DOE. Yet according the NERC annual reliability reports, there were no cybersecurity incidents during the same period.

3. Physical security requirements for the electric grid—and their enforcement—are largely non-existent 6 years after the Metcalf attack.

- *The physical security standard itself—CIP-014-2 (Physical Security)—is inadequate.* There is no requirement that an entity's risk assessment or physical security plan be reviewed by anyone other than a peer utility. There is no regulator determination whatsoever as to the effectiveness of any entity's physical security plan.

- Enforcement of CIP-014-2 (Physical Security) seems nonexistent: In the six years since the Metcalf California substation attack, there have been only four citations issued for violations of the physical security standards. And these four citations were for administrative violations.

4. Cybersecurity Standards Remain Inadequate:

- Despite the fact that the malware is what took down the electric gird in the Ukraine in 2015 and 2016, there remains no requirement that malware in the North American electric grid be detected, mitigated and removed.

- The electric utility industry, including industry lobbyist Edison Electric Institute—whose members include the government of the People's Republic of China[1]—continue to push back against additional cybersecurity measures, claiming that additional cybersecurity protections would be "unduly burdensome" and "unnecessary." And in its rulemaking, the Federal Energy Regulatory Commission bought this argument.

- Congress and the Government Accountability Office (GAO) pointed out deficiencies in cybersecurity in 2008. Congress and the Government Accountability Office (GAO) pointed out *almost identical deficiencies in cybersecurity in 2019*. In other words, we have gone literally nowhere in 11 years.

5. Systematic and Permanent Coverup of Identities of Regulatory Violators:

- Since July of 2010, the identity of every violator of Critical Infrastructure Protection (CIP) standards has been withheld from the public, investors, state regulators and Congress. As of this writing, there have been a total of 256 FERC dockets involving almost 1,500 regulatory violators covered up. FOIA requests have succeeded in uncovering the identity of less than 10 violators.

- The industry, enabled by NERC, has attempted to permanently withhold these names of the violators despite the fact that the violations in most cases have been mitigated long ago.

---

[1] See report: "Is Edison Electric Institute Helping China Lobby For Less Grid Security?" https://michaelmabee.info/edison-electric-institute-china/ (accessed October 19, 2019).

These four interrelated areas of concern point to systematic, pervasive flaws in the regulation and protection of the electric grid. Critical information is being withheld from the public and conflicting (and misleading) information is being disseminated by the government and industry—lulling citizens, investors, state regulators and Congress into a false sense of security.

The details of my research and findings are attached. I hope that NARUC can follow-up and push for actions to improve the regulation of Critical Infrastructure Protection standards.

Sincerely,

Michael Mabee

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Joint Staff White Paper on Notices of	**)**	
Penalty Pertaining to Violations of Critical	**)**	**Docket No. AD19-18-000**
Infrastructure Protection Reliability Standards	**)**	

Comments on the role of transparency in preventing regulatory failures

Submitted to FERC on October 25, 2019

Introduction

I am a private citizen who conducts public interest research on the security of the electric grid because I recognize the absolutely vital role of this infrastructure in powering every one of the nation's 16 critical infrastructures and in undergirding not just the well-being but the very survival of our modern society.

On September 3, 2019 I submitted comments and an alternate proposal to this docket, proposing specific information which should be released to the public by default in CIP Notices of Penalty (NOPs), Spreadsheet Notices of Penalty (SNOPs), "Find, Fix, Track" cases (FFT) and Compliance Exemption (CE) cases. Increased transparency (i.e., the release of the names of CIP standard violators) has been supported in this docket by a wide variety of cybersecurity experts, critical infrastructure protection experts, the press, private citizens and both elected and appointed public officials.

The purpose of this second filing is to provide for the record additional information—all related to transparency—which I believe is critical to this discussion. I have conducted several recent studies which raise significant regulatory red flags about the enforcement of Critical Infrastructure Protection (CIP) standards. I am gravely concerned that the public, investors, Congress and other regulators are receiving inadequate and misleading information about physical security and cybersecurity threats to the electric grid. I am also concerned that the nearly impossible complexity of the regulatory structure puts us at risk.

It is my hope that this docket will inform the public, Congress and other stakeholders as well as ensure that The Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC) and the Department of Energy (DOE) are providing accurate public information on the threats to the electric grid—and what is being done about them. I also hope that this docket sheds light on the complexity, limitations and failings of the current regulatory regime.

If we are to defend the critical energy infrastructure against natural and man-made threats, we must fix this hopelessly complex and bureaucratic "Rube Goldberg" of a regulatory system.

Not surprisingly, the release of the names of CIP violators is vehemently opposed by the industry. The industry is desperately clutching at straws with the vague argument that the release of the names of the violators would somehow help the bad actors attack utilities. This is notwithstanding the fact that the names of all NERC regulated entities are published on its website,[1] so the bad guys already have a target list. Thus, the industry's argument is in essence that we need to protect the names of companies that violate CIP standards—rather than correct the underlying corporate misbehavior (i.e., "security by obscurity" which is a largely discredited security method).

However, the fact is that the public—and the national security of the U.S.—is already in grave danger under the present regulatory regime. The industry's longstanding cover-up of the names of the CIP violators has not made us safer. We need transparency and accountability if the longstanding vulnerabilities of our electric grid are to be adequately addressed.

Finally, the regulatory structure of the "electric grid" is mind-numbingly complex: there are more than 60 state and federal government regulators plus the nonprofit NERC and its seven Regional Entities. The FERC view of what constitutes the "electric grid" is likely limited to the "Bulk Power System" (BPS), however the public and the national security view includes all aspects of generation, transmission and distribution of electric power. Entities often overlap into generation, transmission and distribution; thus, many entities have multiple regulators at the state and federal level. The security needs of the *entire system* must be the focus, which underscores the mandate for transparency surrounding security violators anywhere in that system.

Regulatory Red Flags

As detailed below, my research has uncovered the following four areas of concern. All four are all related to the lack of transparency in the current regulatory regime and should be of great interest to the public, investors, state regulators and Congress:

1. Vast Disparities Exist in Electric Grid Incident Reporting Among Official Sources.

- *Physical Attacks:* There were 578 physical attacks against the grid reported to the Department of Energy from January 1, 2010 through May 31, 2019. Yet according the NERC annual reliability reports, there was only one during the same period.

- *Cyber Attacks:* There were 29 cyberattacks against the grid reported to the Department of Energy (DOE) from January 1, 2010 through May 31, 2019. The Department of Homeland Security (DHS) reports substantially higher numbers of attacks per year than DOE. Yet according the NERC annual reliability reports, there were no cybersecurity incidents during the same period.

[1] See "NCR Active Entities List" https://www.nerc.com/pa/comp/Pages/Registration.aspx (accessed October 19, 2019).

3. Physical security requirements for the electric grid—and their enforcement—are largely non-existent 6 years after the Metcalf attack.

- *The physical security standard itself—CIP-014-2 (Physical Security)—is inadequate.* There is no requirement that an entity's risk assessment or physical security plan be reviewed by anyone other than a peer utility. There is no regulator determination whatsoever as to the effectiveness of any entity's physical security plan.

- Enforcement of CIP-014-2 (Physical Security) seems nonexistent: In the six years since the Metcalf California substation attack, there have been only four citations issued for violations of the physical security standards. And these four citations were for administrative violations.

4. Cybersecurity Standards Remain Inadequate:

- Despite the fact that the malware is what took down the electric gird in the Ukraine in 2015 and 2016, there remains no requirement that malware in the North American electric grid be detected, mitigated and removed.

- The electric utility industry, including industry lobbyist Edison Electric Institute—whose members include the government of the People's Republic of China[2]—continue to push back against additional cybersecurity measures, claiming that additional cybersecurity protections would be "unduly burdensome" and "unnecessary." And in its rulemaking, the Federal Energy Regulatory Commission bought this argument.

- Congress and the Government Accountability Office (GAO) pointed out deficiencies in cybersecurity in 2008. Congress and the Government Accountability Office (GAO) pointed out *almost identical deficiencies in cybersecurity in 2019*. In other words, we have gone literally nowhere in 11 years.

5. Systematic and Permanent Coverup of Identities of Regulatory Violators:

- Since July of 2010, the identity of every violator of Critical Infrastructure Protection (CIP) standards has been withheld from the public, investors, state regulators and Congress. As of this writing, there have been a total of 256 FERC dockets involving almost 1,500 regulatory violators covered up. FOIA requests have succeeded in uncovering the identity of less than 10 violators.

- The industry, enabled by NERC, has attempted to permanently withhold these names of the violators despite the fact that the violations in most cases have been mitigated long ago.

These four interrelated areas of concern point to systematic, pervasive flaws in the regulation and protection of the electric grid. Critical information is being withheld from the public and conflicting (and misleading) information is being disseminated by the government and industry—lulling citizens, investors, state regulators and Congress into a false sense of security.

---

[2] See report: "Is Edison Electric Institute Helping China Lobby For Less Grid Security?" https://michaelmabee.info/edison-electric-institute-china/ (accessed October 19, 2019).

The above summary statements are based on my analysis of the publicly available information, detailed below. To the extent that the Commission or NERC believes that any of the information in the above summary is inaccurate or mischaracterized—perhaps this shows the need for this docket. More transparency would inform the public, investors, Congress and other regulators that all is well—or not.

1. Vast Disparities Exist in Electric Grid Incident Reporting Among Official Sources.

Utility companies and grid operators are required to submit reports on electric disturbance events to the Department of Energy (DOE) on a Form OE-417 ("Electric Emergency Incident and Disturbance Report").

I did an analysis of all the publicly available OE-417 data from 2010 through May of 2019. (I started in 2010 because that is when the NERC CIP Coverup began.[3]) First of all, there were 166 different "event types" reported many of which were either duplicates or related. For example, there were at least 24 different "event types" that denoted a physical attack. There were at least 50 "event types" that denoted a disturbance caused by weather. I grouped these 166 "event types" into 15 categories (actually "causes") so that we could get a sense of what has actually threatened the electric grid in the past 8 1/2 years.

There have been a total of 1,766 electric disturbance events filed during the period of January 1, 2010 through May 31, 2019.

Unfortunately, the public OE-417 data is so bad that there were 251 electric disturbance events where I was unable to identify a cause (14% of the reports). These are highlighted in yellow in the chart. Also, there were 68 generation, transmission and distribution interruptions I was not able to distill down further into what caused the "interruptions." Therefore, there were a total of 319 electric disturbance events (18%) where I couldn't identify the cause. I was able to identify a cause in 1447 electric disturbance events, or 82% of the OE-417 reports filed. (I used this 1447 known population for the study below.)

Event	#
Weather	749
Cyber Attack	29
Physical Attack	578
Fuel Supply Deficiency	61
Equipment	15
Natural Disaster	10
Wildfire	5
Generation Interruption	16
Transmission Interruption	46
Distribution Interruption	6
Operations	80
Islanding	67
Load Shed	30
Public Appeal	64
?	10
Total Reports	**1766**
Cause Known from OE-417	**1447**

The results are disturbing to say the least.

Weather: As one might suspect, weather was the cause of the majority of the disturbances, 749 events, or 52%. If one believes that weather is getting worse in recent years, then this number should be of great concern.

Physical Attacks: Shockingly, there were 578 physical attacks on the grid, or 40% of the incidents. As I will cover in more detail below, the "physical security standards" for our electric grid are weak to begin with and enforcement is almost non-existent.[4]

[3] See Section 4 of this filing below. Full report available at https://michaelmabee.info/nerc-coverup-investigation-report/ (accessed October 25, 2019).

[4] See Section 2 of this filing below. Full report available at https://michaelmabee.info/physical-security-dirty-little-secret/ (accessed October 21, 2019).

Fuel Supply Deficiency: There were 61 events, or 4% of the events. related to fuel supply deficiency. With the retirement of coal and nuclear plants, there is great potential for this problem to get worse.

Cyber Attacks: I was also surprised to learn that there have been 29 cyber attacks reported during this period (2% of the reports). What is most disturbing is that during the same period, the North American Electric Reliability Corporation (NERC) annual reliability reports seem to paint a completely different picture. [5]

OE-417 vs. NERC Reliability Reports

Here is what NERC reported in their annual reports[6] during this same period (note that the report each year is on the previous year, e.g., the 2019 report is for the events of the year 2018):

- **2019 Report** (page ix): "In 2018, there were no reported cyber or physical security incidents that resulted in an unauthorized control action or loss of load."
- **2018 Report** (page viii): "In 2017, there were no reported cyber or physical security incidents that resulted in a loss of load."
- **2017 Report** (page 3): "In 2016, there were no reported cyber or physical security incidents that resulted in a loss of load."
- **2016 Report** (page v): "In 2015, there were no reported cybersecurity incidents that resulted in loss of load. There was one physical security incident that resulted in a loss of approximately 20 MW of load."
- **2015 Report** (page 7): "[N]o Reportable Cyber Security Incidents or physical security reportable events resulted in loss of load on the BPS in 2014." (Misleading, since the Nogales Station in Arizona was attacked by an IED in 2014. [7])
- **2014 Report**: No mention of cyber or physical attacks. (Misleading, since the Metcalf Transformer attack took place in 2013.[8])
- **2013 Report**: No mention of cyber or physical attacks.
- **2012 Report**: No mention of cyber or physical attacks.
- **2011 Report**: No mention of cyber or physical attacks.

There is clearly a huge disconnect between what the industry defines as a cybersecurity or physical security incident and what is reported on the OE-417s. The below chart reproduces the public OE-417 entries for the Metcalf attack (2013), the Nogales attack (2014) and the Buckskin attack (2016):

---

[5] See Section 3 of this filing below.

[6] Available at https://www.nerc.com/pa/RAPA/PA/Pages/default.aspx (accessed October 21, 2019).

[7] Holstege, Sean and Randazzo, Ryan, The Republic. *"Sabotage at Nogales station puts focus on threats to grid."* June 13, 2014. https://www.azcentral.com/story/news/arizona/2014/06/12/sabotage-nogales-station-puts-focus-threats-grid/10408053/ (accessed October 24, 2019).

[8] Smith, Rebecca. The Wall Street Journal. *"Assault on California Power Station Raises Alarm on Potential for Terrorism."* February 5, 2014. https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879 (accessed October 24, 2019).

Date Event Began	Time Event Began	Date of Restoration	Time of Restoration	Area Affected	NERC Region	Alert Criteria	Event Type	Demand Loss (MW)	Number of Customers Affected
4/16/2013	1:47 AM	4/18/2013	3:25 PM	California	WECC		Loss of Part of a High Voltage Substation, Physical Attack	N/A	0
6/11/2014	9:30 AM	6/11/2014	9:31 AM	Nogales, Arizona	WECC		Suspected Physical Attack	N/A	N/A
9/25/2016	12:49 PM	9/25/2016	6:20 PM	Utah: Kane County, Garfield County; Arizona: Coconino County, Mohave County	WECC	Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems	Vandalism	20	10000

While this minimal information was reported on the OE-417, NERC did not find any of it noteworthy enough for their annual reports. These three events were significant physical attacks against the grid which NERC chose not to disclose to the public.

The discrepancies in physical security and cybersecurity reporting can be summarized as follows:

- There were 578 physical attacks against the grid reported on the OE-417's between January 1, 2010 through May 31, 2019, yet according the NERC there was only one during the same period.

- There were 29 cyberattacks against the grid reported on the OE-417's between January 1, 2010 through May 31, 2019, yet according the NERC there were none during the same period.

Meanwhile, federal government reports on cyberattacks against the energy sector during the same periods paint a completely different picture. For example, here's what the United States Government Accountability Office (GAO) had to say in Congressional testimony on October 21, 2015 on cyberattacks:

> "Cyber incidents continue to affect the electric industry. For example, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team noted that the number of reported cyber incidents affecting control systems of companies in the electricity subsector increased from 3 in 2009 to 25 in 2011. The response team reported that the energy sector, which includes the electricity subsector, led all others in fiscal year 2014 with 79 reported incidents. Reported incidents affecting the electricity subsector have had a variety of impacts, including hacks into smart meters to steal power, failure in control systems devices requiring power plants to be shut down, and malicious software disabling safety monitoring systems."

And the U.S. Department of Homeland Security reported 59 cyberattacks on the energy sector in FY 2016[9] and 46 cyberattacks in FY 2015.[10]

Yet NERC reported no cybersecurity incidents in their annual reliability reports for the same periods.

---

[9] National Cybersecurity and Communications Integration Center. "FY 2016 Incidents by Sector." https://www.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf (accessed October 20, 2019).

[10] Idaho National Laboratory. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." August 2016. https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf (accessed October 20, 2019).

NERC's definitions apparently don't consider most cyberattacks to be "reportable cyberattacks", the public is confused when the U.S. government reports a substantial number of cyberattacks against the energy subsector and NERC reports no cyberattacks.

While the industry may argue that there are different populations of regulated entities covered by the various reports, clearly, more transparency is needed for the public, investors, Congress and other regulators to understand these discrepancies and make sense of this conflicting information. Regulatory complexity requires even better public information. More on that later.

2. Physical security requirements for the electric grid—and their enforcement—are largely non-existent 6 years after the Metcalf attack.

At approximately 1:00 a.m. on April 16, 2013, a major PG&E transformer substation in Metcalf California was attacked. The attack was well-planned and sophisticated.[11] One year later, the Metcalf station was struck again when the fence was cut open and, the facility entered and tools were stolen.[12]

Obviously, the physical security situation had not improved much in the intervening year. In fact, PG&E's credibility was shot when its public statements about its physical security improvements were contradicted by a leaked internal memo.[13]

The April 2013 Metcalf attack was not the only physical attack on critical components of the North American electric grid. As previously noted, according the Department of Energy OE-417 reports, there were 578 physical attacks against the grid reported from January 1, 2010 through May 31, 2019.

However, the attack on the Metcalf substation—and the other attacks—shouldn't have been a surprise. A year before the Metcalf attack, the National Academies published a report titled: *Terrorism and the Electric Power Delivery System*.[14] The report discussed physical security of high-voltage transformers noting:

> "High-voltage transformers are of particular concern because they are vulnerable to attack, both from within and from outside the substation where they are located. These transformers are very large, difficult to move, custom-built, and difficult to replace. Most are no longer made in the United States, and the delivery time for new ones can run to months or years."

Then, one year after the Metcalf attack, the Wall Street Journal ran two alarming stories:

---

[11] Smith, Rebecca. The Wall Street Journal. *"Assault on California Power Station Raises Alarm on Potential for Terrorism."* February 5, 2014. https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879 (accessed August 9, 2019).

[12] Wald, Matthew L. The New York Times "California Power Substation Attacked in 2013 Is Struck Again." August 28, 2014. https://www.nytimes.com/2014/08/29/us/california-power-substation-attacked-in-2013-is-hit-again.html (accessed October 25, 2019).

[13] NBC Bay Area "Internal Memo Reveals PG&E Years Away from Substation Security." April 5, 2016 https://www.nbcbayarea.com/investigations/Internal-Memo-Reveals-PGE-Years-Away-from-Substation-Security-303833811.html (accessed October 25, 2019).

[14] Available at: https://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system (accessed October 25, 2019).

- Assault on California Power Station Raises Alarm on Potential for Terrorism. *April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid.*[15]

- U.S. Risks National Blackout From Small-Scale Attack. *Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage.*[16]

What was done?

After the February 5, 2014 Wall Street Journal article, the Senate sent a letter on February 7, 2014 to the Federal Energy Regulatory Commission (FERC), to ask them what they were doing to protect the grid.[17] And FERC Responded on February 11, 2014 telling the Senate that:

> "Since the attack on the Metcalf facility in April 2013, the Commission's staff has taken responsive action together with NERC, other federal and state agencies, and transmission and generation asset owners and operators."[18]

Notwithstanding FERC's assurances to the senate in 2014, the physical security of our critical transformers and facilities remains a complete mess in 2019.

Problem #1: The standard—CIP-014-2 (Physical Security)—is a hollow standard.

As a result of Metcalf, FERC ordered NERC to develop a physical security standard. NERC submitted their proposed standard (known as CIP-014-1[19]) on May 23, 2014.

FERC issued an order on November 20, 2014[20] literally ordering NERC to change one word. (The word was: "widespread" and was used 30 times in the proposed standard. This word—a slight of pen by NERC's attorneys—would have excluded many facilities from falling under the standard.)

On October 2, 2015, FERC approved the "Physical Security" standard, known as CIP-014-2.[21] Unfortunately, the physical security standard requires very little:

1. Requirement 1: Each Transmission Owner shall perform a risk assessment of its Transmission stations and Transmission substations.
2. Requirement 2: Each Transmission Owner shall have an unaffiliated third party verify the risk assessment *[e.g., a peer grid company would meet the requirement—"Hey, if you verify mine, I'll verify yours"].*

---

[15] Smith, Rebecca. Wall Street Journal. February 5, 2014. Available at: https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879 (accessed October 25, 2019).
[16] Smith, Rebecca. Wall Street Journal. March 12, 2014. Available at: https://www.wsj.com/articles/u-s-risks-national-blackout-from-small-scale-attack-1394664965 (accessed October 25, 2019).
[17] Available at: https://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-incoming.pdf (accessed October 25, 2019).
[18] Available at: https://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-feinstein.pdf (accessed October 25, 2019).
[19] Available at: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-014-1.pdf (accessed October 25, 2019).
[20] Available at: https://www.ferc.gov/whats-new/comm-meet/2014/112014/E-4.pdf (accessed October 25, 2019).
[21] Available at: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-014-2.pdf (accessed October 25, 2019).

3. Requirement 3: If a Transmission Owner operationally controls an identified Transmission station or Transmission substation, it must notify the Transmission Operator that has operational control of the primary control center.
4. Requirement 4: Each Transmission Owner shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s).
5. Requirement 5: Each Transmission Owner shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s).
6. Requirement 6: Each Transmission Owner shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) under Requirement R5 *[again, a peer grid company would meet the requirement].*

That's it. All the infrastructure owner must do is to have a binder with a bunch of papers labeled "Physical Security Plan" and have any peer utility they choose review the "risk assessment," "evaluation" and "security plan(s)". No need for it to be anybody who knows anything significant about physical security.

And there is no requirement as to what the "Physical Security Plan" must include—or even that it be effective. Nobody with regulatory authority even has to even approve it—All you need is somebody to "review" it. What if the "reviewer" happens to say "this plan sucks?" It doesn't matter. The only requirement is that the three-ring binder be "reviewed." (I guess most any papers in a three-ring binder will do.)

That unapproved three-ring binder of papers is what is standing between the United States and a catastrophic widespread power outage caused by a terrorist attack. (Also, it is worthy of note that generation plants are not included in NERC's physical security standard!)

Problem #2: Enforcement of CIP-014-2 seems nonexistent

One would think that after the public and Congressional interest in the Metcalf attack, FERC and NERC would take a special interest in the enforcement of the physical security standards. Unfortunately, one would be wrong. How many times since Metcalf have utilities been cited for violations of standard CIP-014-2?

Four.

We have had 578 physical attacks to the grid (that have been publicly disclosed) yet, utilities have been cited for violations of the standard only four (4) times in the six (6) plus years since the Metcalf attack. It would appear that this standard and regulatory scheme are not working. Here are the facts.

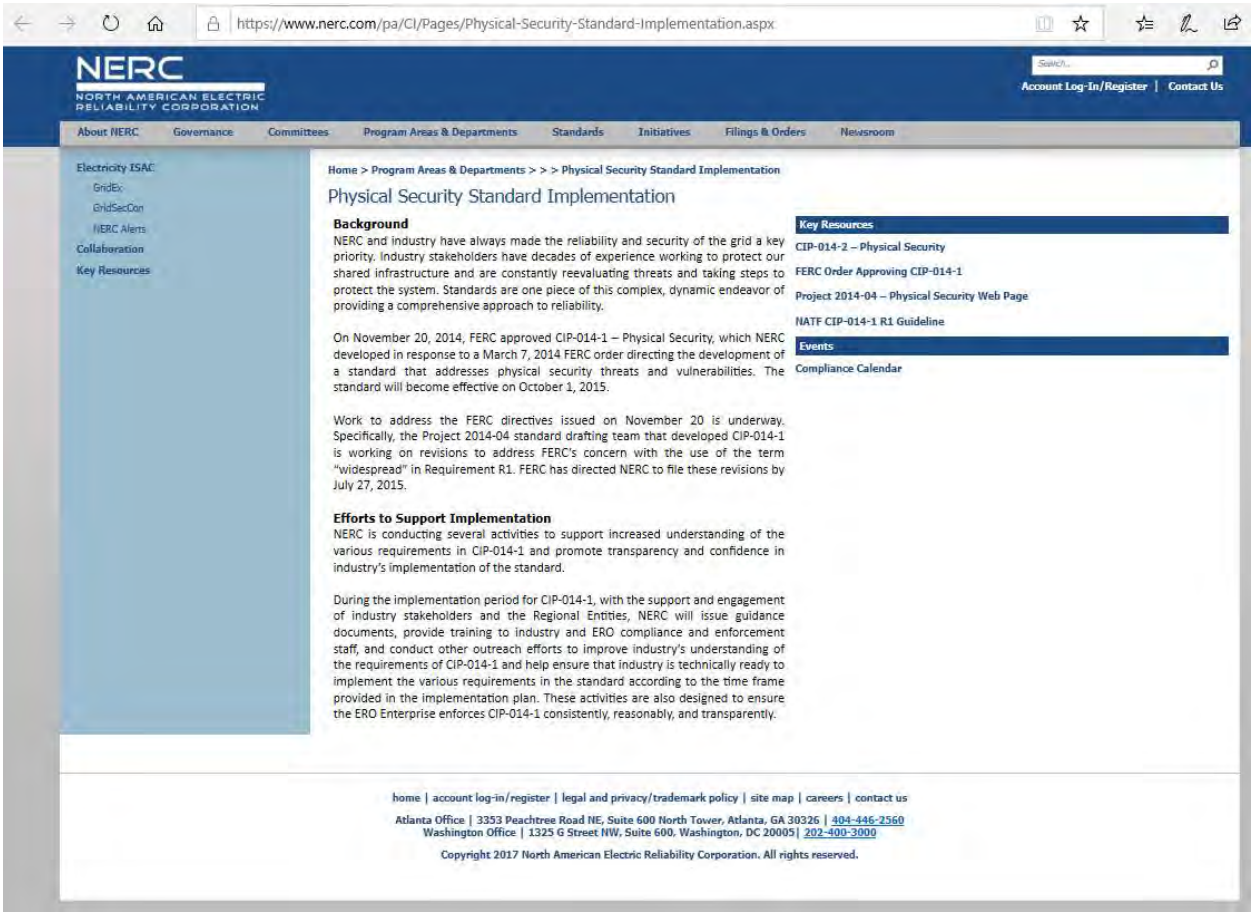
- There are 1,500 entities regulated by NERC.
- There are over 2000 EHV LPTs[22] (Extra High Voltage Large Power Transformers) in the United States and tens of thousands of LPTs.

[22] U.S. Department of Energy "Large Power Transformers and the U.S. Electric Grid." June 2012. https://www.energy.gov/sites/prod/files/Large Power Transformer Study - June 2012_0.pdf (accessed October 25, 2019).

- There have been four (4) citations for non-compliance with the physical security "standards" since Metcalf.

The American people are not stupid. We see these transformers unguarded behind chain-link fences as we drive up the road or walk our dogs.

So how seriously does NERC take physical security? Not very seriously judging by their lack of effort to update their website. Here is a screenshot of NERC's website[23] on "Physical Security" taken on October 18, 2019. The webpage is talking about CIP-014-1. This standard has been superseded since October 2, 2015.



Oh, and that one link you see to "CIP-014-2 – Physical Security" on the right? It leads to an older version of the standard that notes on the last page: "This standard has not yet been approved by the applicable regulatory authority."[24]

---

[23] Screenshot taken on October 18, 2019 of URL: https://www.nerc.com/pa/CI/Pages/Physical-Security-Standard-Implementation.aspx.

[24] I downloaded a copy of this document on October 24, 2019 and it is preserved here: https://michaelmabee.info/wp-content/uploads/2019/10/Older-CIP-014-2-standard-dowloaded-on-2019-10-24.pdf

NERC's physical security webpage does not look as if it has been updated in almost 4 years. What does that tell us about NERC management? (When I wrote an article about this issue exactly six months ago, I had hoped that perhaps NERC would take notice and update their webpage. I should not be surprised that it remains now just as I found it back then.)

So, let's take a look at the four times NERC found CIP-014-2 violations:

- In FERC Docket No. NP19-4-000[25] (one Violation—which everybody knows is Duke Energy Corp. [26]), Duke apparently excluded one substation from its risk assessment because they didn't think it met the criteria for inclusion.
- In FERC Docket No. NP18-14-000[27] (one violation), the "Unidentified Registered Entity" failed to do a risk assessment on one substation due to a "management oopsy."
- And in FERC Docket No. NP17-29-000[28] (two violations), the "Unidentified Registered Entity" failed to include one control center in its 1) risk assessment and 2) security plan (two violations) because an employee who knew what they were doing left the company, leaving nobody else at the company who knew what they were doing.

One will notice that all four of these "violations" are administrative in nature and have nothing to do with whether there is actually meaningful physical security in place.

History of the "Physical Security" standards

CIP-001-1 (Sabotage Reporting)[29] became effective on June 4, 2007. Utilities were cited for its violation 404 times between 6/4/2008 and 5/26/2011. It them morphed into CIP-001-1a (February 2, 2011)[30] and CIP-001-2a (August 2, 2011)[31]—neither of which were EVER cited.

Meanwhile, EOP-004-1 (Disturbance Reporting)[32], which covered "equipment damage" among other things, had violations 16 times between 2009 and 2013.

NERC began to look at merging CIP-001 and EOP-004 "to eliminate redundancies" and on June 20, 2013, FERC approved[33] merging CIP-001-2a (Sabotage Reporting) and EOP-004-1 (Disturbance Reporting) into EOP-004-2 (Event Reporting)[34]. (CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting were then "Retired.") EOP-004-2 covers reporting "damage or destruction of a facility." EOP-004-2 and its successors have never been found to be violated.

Here is the enforcement history of these various standards:

---

[25] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14739324 (accessed October 25, 2019).
[26] Sobczak, Blake and Behr, Peter. E&E News. "Duke agreed to pay record fine for lax security — sources." February 1, 2019. https://www.eenews.net/stories/1060119265 (accessed October 25, 2019).
[27] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14675460 (accessed October 25, 2019).
[28] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14605551 (accessed October 25, 2019).
[29] Available at: https://www.nerc.com/files/CIP-001-1.pdf (accessed October 25, 2019).
[30] Available at: https://www.nerc.com/files/CIP-001-1a.pdf (accessed October 25, 2019).
[31] Available at: https://www.nerc.com/files/CIP-001-2a.pdf (accessed October 25, 2019).
[32] Available at: https://www.nerc.com/files/EOP-004-1.pdf (accessed October 25, 2019).
[33] FERC Order Approving Reliability Standard. 143 FERC ¶ 61,252. https://www.ferc.gov/whats-new/comm-meet/2013/062013/E-8.pdf (accessed October 25, 2019).
[34] Available at: https://www.nerc.com/files/EOP-004-2.pdf (accessed October 25, 2019).

- 404 Citations issued for CIP-001-1 (Sabotage Reporting) between 2008 and 2011
- 16 Citations were issued for EOP-004-1 (Disturbance Reporting) between 2009 and 2013—not all related to damage.

Metcalf happened on April 16, 2013, but then…

- No citations have been issued for EOP-004-2 (effective June 20, 2013)
- No citations have been issued for EOP-004-3 (effective November 19, 2015)
- No citations have been issued for EOP-004-4 (effective January 18, 2018)

And adding in the CIP-014 physical security Standard:

- No violation citations have been issued for CIP-014-1
- Four violation citations have been issued for CIP-014-2
  - NP19-4-000 (one violation)
  - NP18-14-000 (one violation)
  - NP17-29-000 (two violations)

I emphasize: There have been only four (4) NERC Physical Security standard violations cited since the Metcalf attack.

3. Cybersecurity Standards Remain Inadequate:

We know from open sources that state actors such as Russia and China have penetrated the U.S. electric grid for over a decade.

Ten years ago, on April 8, 2009 the *Wall Street Journal* published an article entitled "Electricity Grid in U.S. Penetrated By Spies" in which it was reported:[35]

> 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."

On January 10, 2019—10 years later—the *Wall Street Journal* published an article entitled "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It." The article reports:[36]

---

[35] Available at: https://www.wsj.com/articles/SB123914805204099085 (accessed October 19, 2019).
[36] Available at: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112 (accessed October 19, 2019).

> A reconstruction of the hack reveals a glaring vulnerability at the heart of the country's electric system. Rather than strike the utilities head on, the hackers went after the system's unprotected underbelly—hundreds of contractors and subcontractors like All-Ways who had no reason to be on high alert against foreign agents. From these tiny footholds, the hackers worked their way up the supply chain. Some experts believe two dozen or more utilities ultimately were breached.

Despite the fact that Russia and China have been probing the grid and likely planting malware for over a decade, presently, there is no requirement for malware detection, mitigation and removal. In fact, FERC declined to direct NERC to develop such a standard on December 28, 2017:[37]

> "The Foundation for Resilient Societies filed a petition asking the Commission to require additional measures for malware detection, mitigation, removal and reporting. We decline to propose additional Reliability Standard measures at this time for malware detection, mitigation and removal, based on the scope of existing Reliability Standards, Commission- directed improvements already being developed and other ongoing efforts. However, we propose to direct broader reporting requirements. Currently, incidents must be reported only if they have 'compromised or disrupted one or more reliability tasks,' and we propose to require reporting of certain incidents even before they have caused such harm or if they did not themselves cause any harm." [Emphasis added.]

Russian malware is what took down the electric gird in the Ukraine in 2015[38] and 2016[39]. And yet, there is no requirement for malware detection, mitigation and removal in the U.S. electric grid? This doesn't even make sense.

So, on December 28, 2017 the Commission declined "to propose additional Reliability Standard measures at this time for malware detection, mitigation and removal, based on the scope of existing Reliability Standards, Commission- directed improvements already being developed and other ongoing efforts."

It sounds from this statement like there could be some non-public things going on to protect us. Therefore, the public should "move along—nothing to see here."

Fast forward to the February 14, 2019 Senate Committee on Energy and Natural Resources hearing entitled: "Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry."[40]

---

[37] Proposed Rule "Cyber Security Incident Reporting Reliability Standards." [Docket Nos. RM18–2–000 and AD17–9–000]. Available at: https://www.govinfo.gov/content/pkg/FR-2017-12-28/pdf/2017-28083.pdf (accessed October 19, 2019).

[38] ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure. February 25, 2016. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (accessed October 18, 2019).

[39] Greenberg, Andy. Wired. *'Crash Override': The Malware That Took Down a Power Grid.* June 12, 2017. https://www.wired.com/story/crash-override-malware/ (accessed October 18, 2019).

[40] Available at: https://www.energy.senate.gov/public/index.cfm/hearings-and-business-meetings?ID=FE0534E7-2FC7-4DB0-BEA6-2634D3821ADD# (accessed October 19, 2019).

Over a year after FERC declined to propose Reliability Standard measures for malware detection, mitigation and removal, Senator Angus King questioned NERC CEO James B. Robb on the issue:

> **Sen. King:** "Okay let me ask another question. Do any of our utilities have Kaspersky, Huawei, or ZTE equipment in their system?"
>
> **Mr. Robb:** "We issued a NERC alert…"
>
> **Sen. King:** "I didn't ask you if you issued an alert. I asking you do any of our utilities have ZTE, Huawei, or Kaspersky equipment or software in their system?"
>
> **Mr. Robb:** "Not to my knowledge."
>
> **Sen. King:** "Not to your knowledge. Have you surveyed any of the utilities to determine that?"
>
> **Mr. Robb:** "Uhhh, I don't believe we have."
>
> **Sen. King:** "I think that would be a good idea don't you?"
>
> **Mr. Robb:** "I'll take that on."

In other words, a year later, the regulators hadn't even checked to see if there is Russian or Chinese equipment or software installed on the electric grid.

Meanwhile, the U.S. Government is issuing alerts that the U.S. electric grid is under attack by state actors:

- October 20, 2017 "Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors"[41]
- March 15, 2018 "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors"[42]
- December 20, 2018 "Intrusions Affecting Multiple Victims Across Multiple Sectors"[43]

On January 21, 2021—Four years after the Foundation for Resilient Societies submitted a petition for rulemaking to, among other things, address the lack of a standard to detect, mitigate or remove malware—the modified reliability standard CIP-008-6 (Cyber Security—Incident Reporting and Response Planning) will become effective. The only real improvement will be to incident reporting.

---

[41] US-CERT Alert (TA17-293A) "Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors" October 20, 2017. https://www.us-cert.gov/ncas/alerts/TA17-293A (accessed October 20, 2019).

[42] US-CERT Alert (TA18-074A) "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." March 15, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A (accessed October 20, 2019).

[43] US-CERT Alert (TA17-117A) "Intrusions Affecting Multiple Victims Across Multiple Sectors" December 20, 2018. https://www.us-cert.gov/ncas/alerts/TA17-117A (accessed October 20, 2019).

So, there is still no requirement to detect, mitigate or remove malware. But if a utility bumbles across it, they are at least required to report it—***After January 21, 2021!***

Another disgraceful example of the lack of action on cybersecurity is the Aurora vulnerability—the continuing implications of which are very instructive today. In 2007 the Department of Homeland Security and the Idaho National Laboratory informed the industry[44] about the risk of a cyber-induced "Aurora Vulnerability" which could cause physical damage to grid infrastructure.[45]

Leading cybersecurity experts have been warning about Aurora since 2008[46] and that these experts also consider the cyberattacks in Ukraine as merely a warning[47] due to the fact that the Russian's could have, but chose NOT to exploit the Aurora vulnerability. The Department of Defense spent American taxpayer dollars to help create hardware to mitigate the Aurora vulnerability and offered these Cooper Power Systems iGR-933 Rotating Equipment Isolation Devices (REIDs) *free of charge* to utilities, and despite the fact that NERC ES-ISAC issued an initial Advisory Alert on Aurora in 2007 and another on Oct. 13, 2010, to date, it appears that only *two utilities* have decided to install these mitigation devices while the rest of the devices, which were paid for by U.S. taxpayers, likely collect dust in a warehouse somewhere (hopefully) in the United States.[48]

On May 21, 2008 Representative James R. Langevin, chairman of the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, in his opening statement to a hearing on cybersecurity[49] noted:

> *First, we will receive an update from the Federal Energy Regulatory Commission, FERC, and the North American Electric Reliability Corporation, NERC, about electric industry efforts to mitigate a cyber vulnerability known as Aurora. I think we could search far and wide and not find a more disorganized, ineffective response to an issue of national security of this import. Everything about the way this vulnerability was handled, from press leaks, to DHS's failure to provide more technical details to support the results of its test, to NERC's dismissive attitude to the industry's halfhearted approach toward mitigation, leaves me with little confidence that we are ready or willing to deal with the cybersecurity threat.*

---

[44] See NERC Press Release: "NERC Issues AURORA Alert to Industry." October 14, 2010. https://michaelmabee.info/wp-content/uploads/2019/10/PR_AURORA_14_Oct_10.pdf (accessed October 24, 2019)

[45] Meserve, Jeanne. CNN. "Mouse click could plunge city into darkness, experts say." September 27, 2007. http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html (accessed October 24, 2019)

[46] See Unfettered Blog: "One reason why we need regulation" https://www.controlglobal.com/blogs/unfettered/one-reason-why-we-need-regulation/

[47] See Unfettered Blog: " Waterfall Security podcast on Aurora and the need for engineers" https://www.controlglobal.com/blogs/unfettered/waterfall-security-podcast-on-aurora-and-the-need-for-engineers/ or https://waterfall-security.com/podcasts/joe-weiss (accessed October 24, 2019).

[48] See "What You Need to Know (and Don't) About the AURORA Vulnerability" https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?printmode=1

[49] "Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid." Before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (110th Congress) May 21, 2008. https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg43177/pdf/CHRG-110hhrg43177.pdf (accessed October 24, 2019). Hearing video available at: https://www.c-span.org/video/?205553-1/security-electric-grid (accessed October 24, 2019).

> *As time passes, I grow particularly concerned by NERC, the self-regulating organization responsible for ensuring the reliability of the bulk power system. Not only do they propose cybersecurity standards that, according to the GAO and NIST, are inadequate for protecting critical national infrastructure, but throughout the committee's investigation they continued to provide misleading statements about their oversight of industry efforts to mitigate the Aurora vulnerability.*
>
> *If NERC doesn't start getting serious about national security, it may be time to find a new electric reliability organization. NERC can begin demonstrating its commitment by incorporating more of the NIST security controls in the next iteration of its reliability standards.*

Also, of note, U.S. House Representative Bill Pascrell accused NERC of lying about their cybersecurity follow-up and requested that NERC be held in contempt of Congress.[50]

That hearing was in 2008. So, what is the public to make of the fact that the Government Accountability Office (GAO) issued a report in September of 2019[51] finding:

> *The Federal Energy Regulatory Commission (FERC)—the regulator for the interstate transmission of electricity—has approved mandatory grid cybersecurity standards. However, it has not ensured that those standards fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework.*

Eleven years have elapsed and we are in exactly the same place on cybersecurity as we were in 2008?

Please excuse the public if we are skeptical that "Commission- directed improvements already being developed and other ongoing efforts" are keeping us safe. It does not appear by the testimony in the Congressional Hearings between 2008 and 2019 and the other evidence above (not the least of which is that NERC was caught lying to Congress about cybersecurity already) that FERC and NERC have done enough to protect the grid.

The public needs transparency and accountability to see whether FERC and NERC are up to the task of securing the electric grid from cybersecurity threats. The publicly available evidence indicates they are not.

4. Systematic and Permanent Coverup of Identities of Regulatory Violators:

Since July of 2010, the identity of every violator of Critical Infrastructure Protection (CIP) standards has been withheld from the public, investors, state Public Utility Commissions (PUCs) and Congress. Prior to

---

[50] See Hearing video and record: https://michaelmabee.info/cyber-vulnerabilities-hearing/ (accessed October 24, 2019).

[51] U.S. Government Accountability Office. "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid." GAO-19-332: Published: Aug 26, 2019. Publicly Released: Sep 25, 2019.
https://www.gao.gov/products/GAO-19-332 (accessed October 22, 2019).

this "white paper" docket, NERC and FERC were attempting to permanently withhold the names of the violators despite the fact that the violations in most cases have been long ago mitigated.

I have been conducting an investigation since March of 2018 into NERC's practice of withholding the identities of CIP violators from the public. This investigation has revealed that from July of 2010 through September of 2019 there had been 256 FERC dockets involving almost 1,500 "Unidentified Registered Entities."[52] In each of these instances, the identity of the regulatory violator was withheld from the public.[53] As part of the investigations, I have filed six Freedom of Information Act Requests, three of which are still pending, covering 253 FERC dockets.[54]

We know for a fact from open sources that the Russians and the Chinese have been in our electric grid for over a decade:

- April 8, 2009 Wall Street Journal: "Electricity Grid in U.S. Penetrated By Spies" [55]
- January 10, 2019 Wall Street Journal: "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It." [56]

So, if keeping the names of the CIP violators from the public was going to make us safer, wouldn't it have worked by now? I have concluded that "secret regulation" of CIP standards has not worked. It appears from the available evidence that the real reason for the "protection" of the names of the regulatory violators is because the industry does not want to be held accountable for doing more than the minimum on physical and cyber security. There appears to be no legitimate security reason to withhold the names of regulatory violators in perpetuity as is currently the practice.

Notably the electric utility industry has threatened to stop "self-reporting" violations if FERC begins to release the names of CIP violators. The Trade Associations' Motions to Intervene in FERC Docket No. NP19-4-000[57] contains a not so thinly veiled threat:

> "If the Commission begins releasing entity names in addition to the information already made public in the posted Notices of Penalty, then Registered Entities may re-evaluate whether they will continue to self-report security information knowing that providing such information to their regulators may be disclosed to the public, including to people seeking to attack their systems. In addition, Registered Entities also may re-evaluate what information is included in their mitigation plans."

---

[52] Note: "Unidentified Registered Entity" or "URE" is the industry euphemism for CIP standard violators whose names are being withheld by NERC. As of 2019 NERC began hiding the number of UREs covered in spreadsheet NOPs, so we can no longer accurately determine the number of URE's involved and are making low-end estimates of the number of entities.

[53] A detailed report of the investigation is available here: https://michaelmabee.info/nerc-coverup-investigation-report/ (accessed October 25, 2019). Also see: https://michaelmabee.info/grid-coverup-continues/ (accessed October 25, 2019).

[54] Details, updates and copies of my FOIA requests and responses are available here: https://michaelmabee.info/cip-violation-database/ (accessed October 25, 2019).

[55] Available at: https://www.wsj.com/articles/SB123914805204099085 (accessed October 25, 2019).

[56] Available at: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112 (accessed October 25, 2019).

[57] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14756159 (accessed October 25, 2019).

This is an extraordinary threat that the entire industry represented by the Trade Associations, and who are subject to mandatory reliability standards under federal law,[58] will essentially engage in a regulatory mutiny if the Commission decides to release the names of regulatory violators to the public, as its past orders and regulations require.

The industry is essentially arguing that the names of the regulatory violators constitutes "Critical Electric Infrastructure Information" (CEII) and should be withheld from the public permanently (even after the violations are mitigated). This argument is unsupported by FERC regulations and past FERC orders.[59]

There is a public interest in disclosing the names of regulatory violators because:

- Disclosing the names of the violators might lead the public and Congress to assess how well the regulatory system is working.
- This information would inform the public, investors, PUCs and Congress as to whether the current regulatory system has adequately thwarted threats to the grid.
- This information could lead the public, investors, PUCs and Congress to conclude that better investment in the critical infrastructures is necessary.

These are public policy questions, not CEII.

In sum, CIP regulations should protect the U.S. electric grid by holding the electric utility companies and grid operators accountable to protect the portion of the U.S. critical infrastructure that they own or operate. Instead, the electric utility industry has twisted this regulatory scheme into a sham where companies have no incentive to do more than the minimum. If caught violating a CIP standard, NERC and the Regional Entities will settle the matter privately with the "unidentified registered entities" negotiating a "penalty" that the "unidentified registered entities" are willing to pay and will keep the matter from public view. It looks like a system of back-room settlements and handshake penalties. A great deal for the "unidentified registered entities"—not so much for the American people.

---

[58] 16 U.S. Code § 824o(b)(1) (Electric reliability) provides that: "The Commission shall have jurisdiction, within the United States, over the ERO certified by the Commission under subsection (c), any regional entities, and all users, owners and operators of the bulk-power system, including but not limited to the entities described in section 824(f) of this title, for purposes of approving reliability standards established under this section and enforcing compliance with this section. *All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section*." [Emphasis added.]

[59] For further details, see my Motion to Intervene in FERC Docket NP19-4-000 available at: https://michaelmabee.info/wp-content/uploads/2019/02/FERC-Docket-NP19-4-Motion-to-Intervene-Mabee.pdf (accessed August 12, 2019); Reply Comments in FERC Docket NP19-4-000 available at: https://michaelmabee.info/wp-content/uploads/2019/05/Reply-Comments-of-Michael-Mabee-in-NP19-4-000.pdf (accessed August 12, 2019); Petition for Rulemaking available at: https://michaelmabee.info/wp-content/uploads/2019/02/Petition-for-Rulemaking-Mabee-with-exhibits-1.pdf (accessed August 12, 2019).

The mind-numbing complexity of the regulatory scheme requires transparency (and, likely, reform).

Who regulates the grid? (Spoiler alert: no one)

The North American electric grid is an amazing human accomplishment. It is the largest machine in the history of the world, built piece by piece over many generations. Unfortunately, the regulatory system has also been built piece by piece over the years and today is as overly complex and unwieldy as a Rube Goldberg cartoon. The Federal Energy Regulatory Commission (FERC) has authority only over the "bulk power system" which is largely the interstate transmission system. However, FERC's authority is complicated and indirect: largely the grid is self-regulated through a private corporation—the North American Electric Reliability Corporation (NERC). Again, this is largely just the "bulk power system."

In fact, our electric grid today is regulated by over 60 regulators at the federal and state level as well as a mix of non-governmental non-profit regulators. To further complicate matters, on the federal level alone we have numerous agencies with some degree of interest in protecting the electric grid: FERC, DOE, DHS, NRC and DOD to name a few obvious ones. However, only FERC has any authority over "the electric grid" and FERC's limited authority is only over the Bulk Power System—that portion at 100kV and above.

Each state has its own Public Utility Commission (PUC) which regulates distribution and, in some cases, generation plants. Some generation plants are regulated by other agencies, such as the Nuclear Regulatory Commission (NRC).

So, in the end, no one body regulates "the grid" (i.e., generation, transmission and distribution). Our most critical infrastructure consists of "patchwork" regulation, dependent of scores of agencies, with scores of often conflicting agendas, varying ability (or willingness) to communicate. And most of all, it depends on thousands of companies to do the right thing when there is no strong requirement or incentive for them to do so.

In sum, the present regulatory system is a disaster waiting to happen.

Moreover, many companies transcend regulatory lines. Many companies fall under both FERC/NERC and PUC jurisdiction (and possibly other agencies, such as the NRC).

- State PUC's need to know the identities of the CIP violators because, among other things, state PUC's often control the funding for mitigation.

- Some of these companies may supply critical DOD and DHS facilities. DOD and DHS need to know if companies they are dependent upon to power facilities critical to national security are violating CIP standards.

- Some of these companies may operate nuclear generation plants and fall under the jurisdiction of the NRC as well as FERC/NERC and a PUC (or more than one PUC). These regulators all need to know if the companies they regulate are in violation of CIP standards.

- Some of these companies are also regulated by the Securities Exchange Commission and have reporting requirements for material events. Since the names of CIP violators are being covered up, investors are unaware of the cybersecurity risks that these publicly traded companies face—and whether the "C Suite" is taking appropriate actions to mitigate (*or at least disclose*) investor risk.

It is hard to imagine how such a Balkanized system would function in any context, and clearly it is not functioning efficiently in terms of the CIP red flags previously discussed. And we are talking here about protecting our most critical infrastructure—one in which the lives of 327 million Americans and our very national security depends.

Until the regulatory system is reformed by Congress, disclosure and transparency are critical to our national security. There is no possible way for there to be accountability for the thousands of companies involved in the generation, transmission and distribution of electric power in the U.S. (the whole grid—not just the BPS) except for transparency by FERC and NERC.

Who pays the CIP fines and who pays for mitigation?

If the possibility of hundreds of thousands, if not millions of deaths in a long-term blackout isn't disturbing enough, consider this:

- Who is paying for the CIP violation fines—the ratepayers or the shareholders?
- Who is paying for any mitigation ordered or agreed upon—the ratepayers or the shareholders?
- Most importantly, *who decides who pays*?

The last question is easy: Absent transparency, the regulatory violator decides who pays. This is why it is critical that the Commission release the names of the regulatory violators along with sufficient information so that the public ("ratepayers"), investors ("shareholders"), the PUCs (the ones who should be making these decisions) and Congress (the oversight) can see what is happening.

Last year, PG&E Corp was fined 2.7 million dollars for a cyber breach (which was exposed by one of my Freedom of Information Act requests).[60] PG&E presumably also had to spend an unknown amount (but likely a substantial amount) of money on mitigation. Somebody had to pay for all of this. Because I could find no disclosure of the event or its costs in PG&E's filings with the Securities and Exchange Commission, it is impossible for the public to know whether the shareholders or the ratepayers ate these costs—I am sure both groups would like to know.

Does it make a difference in who should pay if a company is a repeat CIP violator? Does it make a difference in who should pay if the company is negligent?

The *last* one who should be deciding who pays *is the regulatory violator*. This decision should be made by the appropriate regulator (the PUC) with full transparency to the two possible victims: the ratepayers and the shareholders.

[60] See report: https://michaelmabee.info/pge-endangered-the-grid/ (accessed October 22, 2019).

Ratepayers and investors deserve transparency and accountability. PUCs and Congress deserve sufficient information to effectively regulate and govern. Regulatory violators do not deserve reputational protection by the regulators at the expense of the public interest.

Conclusion

The electric grid—including generation, transmission and distribution—is *the most* critical infrastructure as all other critical infrastructures depend on it.

The American people, investors, Congress and other regulators are not getting enough information to evaluate the threats to the electric grid (generation, transmission and distribution), whether there are repeat violators and whether the regulatory regime is effective. There is ample evidence of regulatory red flags and, from the regulators, only a confusing lack of information. We need action by both FERC and Congress:

FERC is the *only agency* in a position to act immediately to address the vulnerabilities to a critical portion of the electric grid (generation and high voltage transmission) that have been created by the industry's desire the keep the names of the CIP violators secret. FERC must decide in the public interest and make increased transparency its policy.

Congress must also act to streamline or revise this overly complex regulatory system and set a federal minimum for critical infrastructure protection for the entire electric grid, including generation, transmission and distribution. We can no longer leave America's Achilles' heel in this inefficient regulatory morass.

Moreover, we can no longer tolerate the fact that keeping our lights on is dependent upon the discretion of Russia and China.

Recommendations:

1. The Commission should adopt my alternate proposal submitted to this docket on September 3, 2019 as the default disclosure for future Notices of Penalty (NOPs), Spreadsheet Notices of Penalty (SNOPs), "Find, Fix Track" cases (FFTs) and Compliance Exemptions (CEs). This alternate proposal would provide sufficient information to the public, investors, Congress and other regulators and would not provide adversaries with actionable information. The alternate proposal has been supported by numerous other commenters on this docket, including internationally renowned security experts.

2. The Department of Energy must enhance the publicly available OE-417 information so that the cause of each reported disturbance and the number of customers affected can be easily discerned.

3. The OE-417s and the NERC annual reliability reports do not tell the American people the same story. NERC's annual reliability reports must address the OE-417 data in order to eliminate this apparent discrepancy. If necessary, The Commission should direct NERC to do this. PUCs will need to be involved, so FERC should suggest that NARUC put this topic on their agenda for immediate action.

4. The Department of Energy Office of the Inspector General should investigate and report on the massive red flags in the enforcement of the physical security standard. Public information indicates that there has been a lack of regulatory action on physical security standards despite the fact that there have been 578 physical attacks against the grid reported from January 1, 2010 through May 31, 2019 according the Department of Energy OE-417 reports. Most disturbingly, NERC has reported only one physical attack in its annual reliability reports over the same period and the violations of the physical security standard have been cited only four times since the Metcalf attack in 2013.

5. The Commission (possibly in collaboration with DOE, DHS, DOD and the National Guard) should "Red Team" utilities in order to evaluate weaknesses and determine whether their cybersecurity and physical security programs are effective. FERC should work with the National Association of Regulatory Utility Commissioners (NARUC) to ensure like actions at the state-level.

6. The Commission should grant the Foundation for Resilient Societies "Motion for the Commission to Hold a Public Hearing" submitted to FERC on October 23, 2019.[61]

7. Congress should set a minimum federal floor for CIP standards for the entire electric infrastructure—not just the "bulk power system."

8. Congress should establish federal regulatory authority for protection of the entire U.S. electric grid—including generation, transmission and distribution.

Respectfully submitted,

Michael Mabee

CC: U.S. Department of Energy—Office of the Inspector General
U.S. Government Accountability Office
U.S. Congresswoman Anne Kuster (NH)
U.S. Senate Committee on Energy and Natural Resources
U.S. House Committee on Energy and Commerce
National Association of Regulatory Utility Commissioners

[61] FERC Accession Number: 20191023-5103 Available at https://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=15388774 (accessed October 24, 2019).