For Immediate Release

Grid Security Investigator Files Complaint Addressing Inadequate Electric Grid Physical Security

Washington DC – Grid Security Investigator Michael Mabee filed a formal complaint with the Federal Energy Regulatory Commission (FERC) charging that the physical security standards and enforcement for the electric grid are inadequate. FERC docketed the complaint and issued a notice on February 6, 2020.

The mandatory physical security standard came about as the result of media attention and Congressional concern about a well-planned and coordinated physical attack on Pacific Gas & Electric's Metcalf transformer substation just outside of San Jose California on April 16, 2013. Often referred to as a "sniper attack," this event initiated a focus on physical security vulnerabilities that led the Federal Energy Regulatory Commission to conclude that such an attack, if successfully executed in just 9 locations across the United States, could blackout the nation for up to 18 months.

However, this was not the first time the Federal Government has reported on physical security vulnerabilities to the nation's bulk power system. U.S. Government Accountability Office reports dating back to at least 1981 discuss the vulnerability of the electric grid to physical attacks.

Nevertheless, Mr. Mabee's research indicates that in 2020, the present standard is inadequate and rarely enforced. Since the Metcalf attack in 2013, the grid's regulator, the North American Electric Reliability Corporation (NERC), has only cited violations of the physical security standard 4 times.

"The April 2013 Metcalf attack was not the only physical attack on critical components of the North American electric grid. 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." Mabee said in his complaint.

Moreover, Mabee argues that the underlying standard is inadequate. "There is no requirement that an entity's risk assessment or physical security plan be reviewed by anyone with any physical security expertise. There is no regulator determination whatsoever as to the effectiveness of any entity's physical security plan." Mabee said in his complaint.

"All a company needs to meet the standard is a three-ring binder of papers labelled 'Physical Security Plan.'" Mabee said. "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."

FERC issued a notice that interested parties have until 5:00 Eastern Time on March 2, 2020 to file motions to intervene and comments. Under the law, FERC can direct NERC to either submit or modify a reliability standard if the Commission considers such a new or modified reliability standard appropriate.

FERC Docket No. EL20-21-000

For further information, contact:

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

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint under Section 215 of the	**)**	
Energy Policy Act of 2005 related to Critical	**)**	**Docket No.** EL20-21-000
Infrastructure Protection Reliability Standards	**)**	

COMPLAINT

Submitted to FERC on January 29, 2020

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.

I am filing this complaint under 16 U.S. Code § 824o(d)(5)[1] and 16 U.S. Code § 824o(e)(3)[2] because it appears from publicly available information that: 1) the mandatory physical security standard is inadequate, and 2) enforcement of the mandatory physical security standard seems nonexistent. In summary:

1. *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 with any physical security expertise. There is no regulator determination whatsoever as to the effectiveness of any entity's physical security plan.

2. *Enforcement of CIP-014-2 (Physical Security) seems nonexistent*. In the almost seven 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.

---

[1] "The Commission, upon its own motion ***or upon complaint***, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section." [Emphasis added.]

[2] "On its own motion ***or upon complaint***, the Commission may order compliance with a reliability standard and may impose a penalty against a user or owner or operator of the bulk-power system if the Commission finds, after notice and opportunity for a hearing, that the user or owner or operator of the bulk-power system has engaged or is about to engage in any acts or practices that constitute or will constitute a violation of a reliability standard." [Emphasis added.]

Request for Investigation

I request that the Commission issue a public notice of this Complaint pursuant to 18 CFR § 385.206(d), investigate this Complaint and issue an appropriate order to the Electric Reliability Organization ("ERO") to correct deficiencies.

Background

Physical security requirements for the electric grid—and their enforcement—are largely non-existent almost 7 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.[3] One year later, the Metcalf station was struck again when the fence was cut open and, the facility entered and tools were stolen.[4]

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.[5]

The April 2013 Metcalf attack was not the only physical attack on critical components of the North American electric grid. 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.[6]

However, the attack on the Metcalf substation—and the other attacks—shouldn't have been a surprise. On May 12, 1981, the General Accounting Office (GAO) issued a report entitled: "Federal Electrical Emergency Preparedness Is Inadequate." GAO noted in 1981:

> "If saboteurs, terrorists, or an enemy attacked the Nation's electric power system, would the Federal Government be prepared to handle the resulting energy disruptions?
>
> Probably not, because the Department of Energy has failed to prepare required electric emergency preparedness plans. A national plan to cope with the problems caused by a loss of electricity–which would virtually halt communication, transportation, and distribution systems–

[3] 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 January 29, 2020).

[4] 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 January 29, 2020).

[5] NBC Bay Area "Internal Memo: PG&E Years Away from Substation Security." May 15, 2015 https://www.nbcbayarea.com/on-air/as-seen-on/internal-memo_-pg_e-years-away-from-substation-security_bay-area/69201/ (accessed January 29, 2020).

[6] See report: "Electric Disturbance Events: What is the public allowed to know?" https://michaelmabee.info/electric-disturbance-events/ (accessed January 29, 2020).

> is essential, because utilities and the States cannot be expected to deal with such emergencies on their own."

At least as far back as 1981, GAO was concerned about the physical security of our substations. GAO found:

> "Electric power systems are highly dependable, but are very vulnerable to disruptions from acts of war, sabotage, or terrorism. In the region GAO looked at:
>
> - An attack on just eight substations could disrupt power to the entire region for a long time. (See p. 8.)
> - Damage to just four substations could disrupt power to one city for up to a year. (See p. 8.)
> - Damage to just one substation could leave a key military facility without power. (See p. 8.)"

Further, a year before the Metcalf attack, the National Academies published a report titled: *Terrorism and the Electric Power Delivery System*.[7] 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:

- Assault on California Power Station Raises Alarm on Potential for Terrorism. *April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid.*[8]

- U.S. Risks National Blackout From Small-Scale Attack. *Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage.*[9]

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.[10] And FERC Responded on February 11, 2014 telling the Senate that:

---

[7] Available at: https://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system (accessed January 29, 2020).
[8] 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 January 29, 2020).
[9] 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 January 29, 2020).
[10] Available at: https://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-incoming.pdf (accessed January 29, 2020).

> "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."[11]

Notwithstanding FERC's assurances to the senate in 2014, the physical security of our critical transformers and facilities appears to remain inadequate in 2020.

Complaint 1. The standard—CIP-014-2 (Physical Security)—is inadequate.

As a result of Metcalf, FERC ordered NERC to develop a physical security standard. NERC submitted their proposed standard (known as CIP-014-1[12]) on May 23, 2014.

FERC issued an order on November 20, 2014[13] 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.[14] 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"].*
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.

---

[11] Available at: https://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-feinstein.pdf (accessed January 29, 2020).
[12] Available at: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-014-1.pdf (accessed January 29, 2020).
[13] Available at: https://www.ferc.gov/whats-new/comm-meet/2014/112014/E-4.pdf (accessed January 29, 2020).
[14] Available at: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-014-2.pdf (accessed January 29, 2020).

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.)

Complaint 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 almost seven (7) years since the Metcalf attack. It would appear that this standard and regulatory scheme are not working. Here are the facts.

- There are close to 1,500 entities regulated by NERC.
- There are over 2000 EHV LPTs[15] (Extra High Voltage Large Power Transformers) in the United States and tens of thousands of LPTs.
- There have been four (4) citations for non-compliance with the physical security standard (CIP-014-2) 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, let's take a look at the four times NERC found CIP-014-2 violations:

- In FERC Docket No. NP19-4-000[16] (one Violation—which everybody knows is Duke Energy Corp. [17]), 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[18] (one violation), the "Unidentified Registered Entity" failed to do a risk assessment on one substation due to a "management oopsy."

---

[15] 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 January 29, 2020).

[16] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14739324 (accessed January 29, 2020).

[17] 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 January 29, 2020).

[18] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14675460 (accessed January 29, 2020).

- And in FERC Docket No. NP17-29-000[19] (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)[20] 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)[21] and CIP-001-2a (August 2, 2011)[22]—neither of which were EVER cited.

Meanwhile, EOP-004-1 (Disturbance Reporting)[23], 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[24] merging CIP-001-2a (Sabotage Reporting) and EOP-004-1 (Disturbance Reporting) into EOP-004-2 (Event Reporting)[25]. (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:

- 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

---

[19] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14605551 (accessed January 29, 2020).
[20] Available at: https://www.nerc.com/files/CIP-001-1.pdf (accessed January 29, 2020).
[21] Available at: https://www.nerc.com/files/CIP-001-1a.pdf (accessed January 29, 2020).
[22] Available at: https://www.nerc.com/files/CIP-001-2a.pdf (accessed January 29, 2020).
[23] Available at: https://www.nerc.com/files/EOP-004-1.pdf (accessed January 29, 2020).
[24] FERC Order Approving Reliability Standard. 143 FERC ¶ 61,252. https://www.ferc.gov/whats-new/comm-meet/2013/062013/E-8.pdf (accessed January 29, 2020).
[25] Available at: https://www.nerc.com/files/EOP-004-2.pdf (accessed January 29, 2020).

- 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.

Conclusion and Recommendations

Publicly available information indicates that: 1) the mandatory physical security standard is inadequate, and 2) enforcement of mandatory physical security standard seems nonexistent. I recommend that FERC take the following actions:

1. FERC should direct NERC to modify CIP-014-2 (Physical Security) to require that the entity's "Physical Security Plan" be effective and receive regulatory approval. The standard should specify that all "risk assessments" "evaluations" and "security plans" should be reviewed by qualified non-affiliated persons with expertise in physical security.

2. FERC should direct NERC to submit to the Commission for approval a compliance and enforcement plan for physical security that would provide meaningful assurances that the regulators and regulated entities are taking seriously their obligations to protect the bulk power system from physical threats.

3. FERC (in collaboration with DOE, DHS, DOD, and the National Guard) should "Red Team" entities in order to evaluate weaknesses and determine whether their physical security (and cybersecurity) programs are effective. FERC should work with state PUCs to ensure like actions at the state-level.

Respectfully submitted,

Michael Mabee

Attachment: 18 CFR § 385.206 Compliance Information

18 CFR § 385.206 Compliance Information

I Michael Mabee, hereby state the following:

18 CFR § 385.206(b) Contents. A complaint must:
(1) Clearly identify the action or inaction which is alleged to violate applicable statutory standards or regulatory requirements;

- Contained in Complaint

(2) Explain how the action or inaction violates applicable statutory standards or regulatory requirements;

- Contained in Complaint

(3) Set forth the business, commercial, economic or other issues presented by the action or inaction as such relate to or affect the complainant;

- A widespread power outage as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(4) Make a good faith effort to quantify the financial impact or burden (if any) created for the complainant as a result of the action or inaction;

- A widespread power outage as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(5) Indicate the practical, operational, or other nonfinancial impacts imposed as a result of the action or inaction, including, where applicable, the environmental, safety or reliability impacts of the action or inaction;

- A widespread power outage as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(6) State whether the issues presented are pending in an existing Commission proceeding or a proceeding in any other forum in which the complainant is a party, and if so, provide an explanation why timely resolution cannot be achieved in that forum;

- I am unaware of any open FERC docket on CIP-014-2

(7) State the specific relief or remedy requested, including any request for stay or extension of time, and the basis for that relief;

- Contained in "Conclusion and Recommendations" section of Complaint.

(8) Include all documents that support the facts in the complaint in possession of, or otherwise attainable by, the complainant, including, but not limited to, contracts and affidavits;

- Records related to the enforcement of CIP-014-2 are in the possession of the Commission and/or the Electric Reliability Organization ("ERO").

(9) State

(i) Whether the Enforcement Hotline, Dispute Resolution Service, tariff-based dispute resolution mechanisms, or other informal dispute resolution procedures were used, or why these procedures were not used;

- N/A

(ii) Whether the complainant believes that alternative dispute resolution (ADR) under the Commission's supervision could successfully resolve the complaint;

- N/A

(iii) What types of ADR procedures could be used; and

- N/A

(iv) Any process that has been agreed on for resolving the complaint.

- N/A

(10) Include a form of notice of the complaint suitable for publication in the Federal Register in accordance with the specifications in § 385.203(d) of this part. The form of notice shall be on electronic media as specified by the Secretary.

- N/A

(11) Explain with respect to requests for Fast Track processing pursuant to section 385.206(h), why the standard processes will not be adequate for expeditiously resolving the complaint.

- N/A

18 CFR § 385.206(c) Service. Any person filing a complaint must serve a copy of the complaint on the respondent, affected regulatory agencies, and others the complainant reasonably knows may be expected to be affected by the complaint. Service must be simultaneous with filing at the Commission for respondents. Simultaneous or overnight service is permissible for other affected entities. Simultaneous service can be accomplished by electronic mail in accordance with § 385.2010(f)(3), facsimile, express delivery, or messenger.

- A copy of this Complaint will be sent electronically to the Electric Reliability Organization ("ERO") simultaneously with my filing with the Commission.

Respectfully submitted,

Michael Mabee

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee
Related to Critical Infrastructure
Reliability Standard

Docket No. EL20-21-000

NOTICE OF COMPLAINT

(February 6, 2020)

Take notice that on January 30, 2020, pursuant to section 215(d) of the Federal Power Act, 16 U.S.C. 824o(d) and Rule 206 of the Federal Energy Regulatory Commission's (Commission) Rules of Practice and Procedure, 18 CFR 385.206 (2019), Michael Mabee, (Complainant) filed a formal complaint alleging that Critical Infrastructure Protection Reliability Standard (CIP-014-2) (physical security) is inadequate, as more fully explained in the complaint.

Complainant certifies that copies of the Complaint were served on the contacts as listed on the Commission's list of Corporate Officials.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211, 385.214). Protests will be considered by the Commission in determining the appropriate action to be taken, but will not serve to make protestants parties to the proceeding. Any person wishing to become a party must file a notice of intervention or motion to intervene, as appropriate. All interventions, or protests must be filed on or before the comment date.

The Commission encourages electronic submission of protests and interventions in lieu of paper using the "eFiling" link at http://www.ferc.gov. Persons unable to file electronically should submit an original and 5 copies of the protest or intervention to the Federal Energy Regulatory Commission, 888 First Street, N.E., Washington, DC 20426.

This filing is accessible on-line at http://www.ferc.gov, using the "eLibrary" link and is available for electronic review in the Commission's Public Reference Room in Washington, DC. There is an "eSubscription" link on the web site that enables subscribers to receive email notification when a document is added to a subscribed

docket(s). For assistance with any FERC Online service, please email FERCOnlineSupport@ferc.gov, or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Comment Date: 5:00 Eastern Time on March 2, 2020.

Kimberly D. Bose,
Secretary.

Document Content(s)