171 FERC ¶ 61,205
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Neil Chatterjee, Chairman;
Richard Glick, Bernard L. McNamee,
and James P. Danly.

Complaint of Michael Mabee
Related to Critical Infrastructure
Reliability Standard

Docket No. EL20-21-000

ORDER DENYING COMPLAINT

(Issued June 9, 2020)

1. On January 29, 2020, as supplemented on February 19, 2020, Michael Mabee filed a complaint (Complaint) under section 215 of the Federal Power Act (FPA)[1] and Rule 206 of the Commission's Rules of Practice and Procedure.[2] The Complaint alleges that Reliability Standard CIP-014-2 (Physical Security) is "inadequate" and "enforcement of the mandatory physical security standard seems nonexistent."[3] The Complaint requests an order from the Commission that directs the North American Electric Reliability Corporation (NERC) to correct these deficiencies. For the reasons discussed below, we deny the Complaint.

I. Background

A. Section 215 and Mandatory Reliability Standards

2. Section 215 of the FPA requires the Commission to certify an Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[4] Once approved, the Reliability Standards are enforceable in the United States by the ERO, subject to Commission oversight, or by the Commission independently. Pursuant to section 215

[1] 16 U.S.C. § 824o (2018).

[2] 18 C.F.R. § 385.206 (2019).

[3] Complaint at 1.

[4] 16 U.S.C. § 824o.

of the FPA, the Commission established a process to select and certify an ERO,[5] and subsequently certified NERC.[6]

B. Reliability Standard CIP-014-2

3. The Commission directed NERC by order on March 7, 2014, pursuant to section 215(d)(5) of the FPA, to develop a physical security Reliability Standard.[7] In Order No. 802, the Commission approved the first version of the Reliability Standard, CIP-014-1, and directed NERC to submit one modification to the Reliability Standard to remove the term "widespread" from the phrase "widespread instability, uncontrolled separation, or Cascading within an Interconnection" from Requirement R1.[8] NERC submitted the modified Reliability Standard in an uncontested filing on May 15, 2015, which was approved on July 14, 2015.[9] Reliability Standard CIP-014-2 is designed to identify and enhance physical security measures for the most critical Bulk-Power System facilities and thereby lessen the overall vulnerability of the Bulk-Power System facilities against physical attacks.

II. Complaint

4. The Complaint, as supplemented, contends that Reliability Standard CIP-014-2 is inadequate because: (1) there is no requirement that physical security plans be effective, approved by a regulatory authority, or reviewed by an entity with physical security expertise; and (2) there is no requirement as to what the physical security plan must include. The Complaint also contends that Reliability Standard CIP-014-2: (1) does not require registered entities to identify critical facilities based on a coordinated attack of

---

[5] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards,* Order No. 672, 114 FERC ¶ 61,104, *order on reh'g,* Order No. 672-A, 114 FERC ¶ 61,328 (2006).

[6] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[7] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014) (March 2014 Order).

[8] *Physical Security Reliability Standard*, Order No. 802, 149 FERC ¶ 61,140, at P 19 (2014), *order on reh'g*, Order Denying Rehearing, 151 FERC ¶ 61,066 (2015).

[9] *North American Electric Reliability Corp.*, Docket No. RD15-4-000 (Jul. 14, 2015) (delegated order).

multiple facilities scenario; (2) does not apply to generator owners and operators or smaller facilities or transmission lines; (3) allows transmission owners to engage in quid pro quo third-party reviews whereby a transmission owner acting as a third-party reviewer would "go easy" on an unaffiliated transmission owner with the expectation of reciprocal treatment; (4) does not require regulatory approval of a transmission owner's documented reasons for not adopting third-party reviewer recommendations; and (5) does not require updated threat and vulnerability evaluations and physical security plans following the initial iteration.

5. The Complaint also contends that the enforcement of Reliability Standard CIP-014-2 "seems nonexistent" because, it alleges, there are only four violations of the Reliability Standard that could be identified. The Complaint asserts that the small number of violations is incongruous with the 245 physical attacks reported to the Department of Energy through the Form OE-417 Electric Emergency Incident and Disturbance Reports since the Reliability Standard became effective.[10]

III. Notice of Filing and Responsive Pleadings

6. Notice of the Complaint was published in the *Federal Register*, 85 Fed. Reg. 7993 (Feb. 12, 2020), with interventions and protests due on or before March 2, 2020. Notice of the February 19, 2020 supplement was published in the *Federal Register*, 85 Fed. Reg. 11,983 (Feb. 28, 2020), with interventions and protests due on or before March 10, 2020. Timely motions to intervene and comments were filed by NERC, Edison Electric Institute (EEI), National Rural Electric Cooperative Association (NRECA), American Public Power Association (APPA), Transmission Access Policy Study Group (TAPS), Large Public Power Council (LPPC), Foundation for Resilient Societies (Resilient Societies), Secure the Grid Association, David K. Testerman, Town of Mount Vernon, Fred A. Reitman, Task Force on National and Homeland Security, Joseph A. Voglund, and Karen Testerman. Timely motions to intervene were filed by Louisiana Public Service Commission, Public Citizen, Inc., American Electric Power Service Cooperation, and Georgia System Operations Corporation.

IV. Answers

7. EEI and NRECA, jointly, TAPS, LPPC, and APPA, jointly, and NERC filed comments in opposition to the assertions contained in the Complaint and the relief sought in the Complaint. These comments contend that: (1) the Commission has already determined that Reliability Standard CIP-014-2 complies with the March 2014 Order and the statutory criteria for approving Reliability Standards set forth in section 215(d)(2) of

[10] On March 28, 2020, complainant filed a motion in this proceeding requesting that the Commission take official notice of two newspaper articles. We have considered this supplemental information in considering the relief sought in the Complaint.

the FPA;[11] (2) the complaint does not contain any new information that would change the Commission's prior determination;[12] (3) the complaint misconstrues the requirements in Reliability Standard CIP-014-2;[13] and (4) the complaint relies on assumptions and inferences that are unsupported or otherwise speculative.[14] Additionally, the comments opposing the Complaint point out that the complainant did not take part in the proceedings leading to the development of Reliability Standard CIP-014-1, did not file comments in the rulemaking proceeding resulting in Order No. 802, and did not seek rehearing of Order No. 802.[15]

8. Secure the Grid Coalition, Task Force on National and Homeland Security, Karen Testerman, David Testerman, Town of Mount Vernon, Cimino, Voglund, and Resilient Societies supported the assertions made in the Complaint and the relief sought in the Complaint.[16]

V. Determination

A. Procedural Matters

9. The unopposed motions to intervene are granted pursuant to the operation of Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2019).

B. Substantive Matters

10. As discussed below, we deny the Complaint because we find that the complainant has not established that Reliability Standard CIP-014-2 is inadequate or unenforced.

---

[11] NERC Comments at 6-7; EEI and NRECA Comments at 4-6.

[12] NERC Comments at 9, 17; EEI and NRECA Comments at 6, 14-15; APPA, LPPC, and TAPS Comments at 3.

[13] EEI and NRECA Comments at 4-5, 7-14.

[14] EEI and NRECA Comments at 17-18; APPA, LPPC, and TAPS Comments at 4-5.

[15] NERC Comments at 10; EEI and NRECA Comments at 15; APPA, LPPC, and TAPS Comments at 3.

[16] Resilient Societies also recommended certain actions to address pandemics that are outside the scope of this proceeding.

1. The Complaint Does Not Establish that Reliability Standard CIP-014-2 is Inadequate

11. In Order No. 802, the Commission found Reliability Standard CIP-014-1 to be just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Complaint provides no new information to justify revisiting that determination or to exercise our authority under section 215(d)(5) of the FPA to direct modifications to the Physical Security Reliability Standard.[17] Instead, as discussed below, the Complaint contains assertions that the Commission addressed and rejected in Order No. 802 and in the Order Denying Rehearing, or it makes new assertions that are either unsupported or misapprehend the requirements in Reliability Standard CIP-014-2.

12. In Order No. 802 and the Order Denying Rehearing, the Commission addressed the Complaint's assertions regarding: (1) the absence of an evaluation of a coordinated attack scenario; (2) the exclusion of generator owners and operators and smaller facilities; and (3) third-party reviews.[18]

13. In the March 2014 Order, the Commission directed NERC to address the physical security of critical facilities, which the Commission defined as "one, that if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."[19] In the Order Denying Rehearing, the Commission stated that the March 2014 Order did not require NERC to address the simultaneous loss of multiple critical facilities. The Commission explained that "[b]y protecting individual critical facilities, responsible entities will necessarily protect critical facilities against simultaneous attacks."[20] The Commission further stated that if the rehearing requester "is seeking to expand the scope of covered facilities to include those not individually critical, we are not prepared to do so at this early stage of industry experience with the new

---

[17] Section 215(d)(5) of the FPA provides that the Commission "may order the Electric Reliability Organization to submit to the Commission . . . a modification to a reliability standard that addresses a specific matter if the Commission considers such a . . . modified reliability standard appropriate to carry out this section." 16 U.S.C. § 824o(d)(5).

[18] NERC observes that the Complaint's recommendations for changes to the Reliability Standard mirror those in Resilient Societies' request for rehearing of Order No. 802, which the Commission rejected in the Order Denying Rehearing. NERC Comments at 10 n.33.

[19] March 2014 Order, 146 FERC ¶ 61,166 at P 6.

[20] Order Denying Rehearing, 151 FERC ¶ 61,066 at P 14.

requirements."[21] The Complaint does not provide any new basis for expanding the scope of the Reliability Standard to include multiple attack scenarios.

14. With respect to the exclusion of generator owners and operators, Order No. 802 agreed with NERC's comments in response to the notice of proposed rulemaking that the exclusion of generator owners and operators is appropriate because "a generation facility does not have the same critical functionality as certain Transmission stations and Transmission substations due to the limited size of generating plants, the availability of other generation capacity connected to the grid, and planned resilience of the transmission system to react to the loss of a generation facility."[22] The Commission affirmed that determination in the Order Denying Rehearing.[23] The Complaint contends that an attack on a generation facility in combination with other events (e.g., an extreme weather event or generator outage) supports making generator owners and operators subject to the Physical Security Reliability Standard. However, as discussed above, Reliability Standard CIP-014-2 is not intended to address multiple physical attack scenarios, let alone attack scenarios involving extreme weather or forced outages. We find no reason to alter the determination in Order No. 802 that the loss of a generation facility does not have the same impact as the loss of certain critical transmission facilities. Similarly, we decline to direct the inclusion of non-critical facilities or transmission lines within the scope of Physical Security Reliability Standard, as suggested in the Complaint.

15. The Complaint also asserts that third-party verification could devolve into a sham if registered entities act in bad faith (i.e., by agreeing to verify each other's compliance documents). But the Complaint offers no evidence that registered entities have engaged, or intend to engage, in bad faith. In Order No. 802, the Commission explained the importance of third-party verification of the list of critical facilities compiled under Requirement R1, the threat and vulnerability evaluation in Requirement R4 and the physical security plan in Requirement R5. The Commission cited NERC's comments in that proceeding indicating that "third-party verification and review will provide another layer of expertise and independence to the identification of critical assets, the evaluation of threats and vulnerabilities, and the development of effective security plans."[24] Moreover, the Commission stated that "the requirements in Reliability Standard CIP-014-1 (i.e., Requirements R2.1 and R6.1) establishing the qualifications for

[21] *Id.*

[22] Order No. 802, 149 FERC ¶ 61,140 at P 99.

[23] Order Denying Rehearing, 151 FERC ¶ 61,066 at P 20.

[24] Order No. 802, 149 FERC ¶ 61,140 at P 77.

third-party verifiers and reviewers are sufficient."[25] We find no reason to conclude that registered entities will abuse this process. Moreover, a sham verification would not benefit the registered entity because, as the Commission stated in Order No. 802, even if a registered entity's list of critical facilities is verified by a third-party under Requirement R2, that "cannot cure an applicable entity's failure to comply with Requirement R1 if it is determined by the compliance enforcement authority that the applicable entity failed to do so."[26]

16. We find the other assertions in the Complaint to be either unsupported or based on a misreading of Reliability Standard CIP-014-2. The Complaint asserts there are no requirements in Reliability Standard CIP-014-2 that require physical security plans to be effective or explain what must be present in a physical security plan. However, this ignores Requirement R5, which identifies mandatory attributes that must be present in physical security plans. And as to effectiveness, Requirement R5.1 states that physical security plans must, among other things, have "[r]esiliency or security measures designed collectively to deter, detect, delay, assess, communicate and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4."

17. The Complaint also misreads Reliability Standard CIP-014-2 to contend that there is no requirement to update threat and vulnerability evaluations under Requirement R4 or physical security plans under Requirement R5 for previously identified critical facilities. Requirement R5.4, however, states that physical security plans must have "[p]rovisions to evaluate evolving physical threats, and their corresponding security measures." Rather than require updates to the threat and vulnerability evaluations on a periodic basis, this provision requires that physical security plan must include provisions for constant, real-time updating. This interpretation is supported by the Guidelines and Technical Basis document appended to the Reliability Standard, which states that a "registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various source . . . [and] should be used to reevaluate or consider changes in the security plan and corresponding security measures."[27]

18. Further, the Complaint mistakenly asserts that there is no regulatory oversight over a registered entity's decision not to adopt a third-party's recommendation. Requirements R2 and R6 make clear that if a third-party makes a recommendation, the registered entity must either follow the recommendation or document the technical basis for not adopting

[25] *Id.* P 86.

[26] *Id.* P 90.

[27] Reliability Standard CIP-014-2, Guideline and Technical Basis at 30.

it. While registered entities must address third-party recommendations, Order No. 802 made clear that Regional Entities, NERC and the Commission retain regulatory oversight. In Order No. 802, the Commission explained that third-parties do not act in an enforcement capacity and "an applicable entity in some cases could be found to be in violation of a requirement even if the applicable entity's actions were verified by a third-party."[28] As the compliance enforcement authority, the Regional Entities, NERC, or the Commission could determine that a registered entity violated the Reliability Standard by not following a verifier's recommendation. Conversely, as we explained in Order No. 802, compliance enforcement authorities could determine that a registered entity's decision to decline to adopt a recommendation is justified if the verifier did not "articulate a reasonable basis for their recommendations."[29]

19. In sum, we find no basis in the Complaint to conclude that Reliability Standard CIP-014-2 is inadequate at this time.

2. The Complaint Does Not Establish that Reliability Standard CIP-014-2 is Not Being Enforced

20. We are not persuaded that Reliability Standard CIP-014-2 is being unenforced based on the Complaint's assertions.[30] Relying solely on the small number of filed violations is not a sufficient basis for us to conclude that Reliability Standard CIP-014-2 is not being enforced when it is equally plausible that the small number of violations could be attributed to industry compliance. Indeed, the Complaint assumes erroneously that every incident reported under Form OE-417 suggests uncited violations of Reliability Standard CIP-014-2. However, there is no evidence how many of these attacks, if any, were against critical facilities subject to Reliability Standard CIP-014-2. Reliability Standard CIP-014-2 does not purport to eliminate all physical attacks; instead, it is designed to protect critical facilities from physical attack.[31]

---

[28] *Id.* P 86.

[29] *Id.* P 87.

[30] While citing section 215(e)(3) of the FPA, the relief sought in the Complaint regarding generic enforcement of Reliability CIP-014-2 is not the type of action contemplated in that section. Rather, section 215(e)(3) of FPA addresses specific instances of noncompliance by registered entities by providing that the Commission "may order compliance with a reliability standard . . . 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." 16 U.S.C. § 824o(e)(3).

[31] As the EEI and NRECA Comments point out, many of the Form OE-417 entries

21. NERC's comments also indicate that, as of January 31, 2020, there have been 16 (not four) instances of noncompliance with Reliability Standard CIP-014-2 and that NERC and the Regional Entities are currently reviewing other instances.[32] NERC's comments also detail multiple compliance activities related to Reliability Standard CIP-014-2 that NERC and the Regional Entities have undertaken.[33]

22. Accordingly, we find no basis in the Complaint to conclude that Reliability Standard CIP-014-2 is not being enforced.

The Commission orders:

We hereby deny the Complaint, as discussed in the body of this order.

By the Commission. Commissioner McNamee is concurring with a separate statement attached.

(S E A L)

Kimberly D. Bose,
Secretary.

in Exhibit A of the Supplemental Complaint are described as "vandalism." Trade Associations Comments at 18 n.26.

[32] NERC Comments at 12.

[33] NERC Comments at 13-14.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee
Related to Critical Infrastructure
Reliability Standard

Docket No. EL20-21-000

(Issued June 9, 2020)

McNAMEE, Commissioner, *concurring*:

1. The Commission's order in this proceeding denies the Complaint alleging that Reliability Standard CIP-014-2 (Physical Security) is "inadequate" and that "enforcement of the mandatory physical security standard seems nonexistent." The order also denies the Complaint's request for an order from the Commission directing the North American Electric Reliability Corporation (NERC) to correct these alleged deficiencies. Though the Commission's reasoning in denying the Complaint is correct as a matter of law, I write separately to encourage NERC, regulated entities and the Commission to continually reassess the security of all assets used for the generation, transmission and distribution of electricity.[1]

Cyber and Physical Threats Are Real

2. The importance of electricity to the security and safety of the American people cannot be overstated. Virtually every aspect of our lives, our businesses, and our society depend on access to reliable and affordable electricity. Therefore, any realized threat to our electric system can have devastating effects on individuals, families, businesses, the economy and the nation. We know this; so do our adversaries.

3. In the summer of 2018, then Director of National Intelligence Dan Coats stated, referencing the attacks on our country of September 11, 2001, that "the warning lights are blinking red again" and "the digital infrastructure that serves this country is literally under attack."[2] We know that this referenced infrastructure includes our bulk power

[1] I recognize that the Commission does not have jurisdiction over the local distribution of electricity or the siting and permitting of generation facilities; but due to the interconnected nature of the electric system, it is important that regulated entities and regulators be cognizant of the fact that threats to any part of the system can be a threat to the entire electrical system.

[2] *See* NATIONAL PUBLIC RADIO, TRANSCRIPT: DAN COATS WARNS OF CONTINUING RUSSIAN CYBERATTACKS (Jul. 18, 2018), https://www.npr.org/2018/07/18/630164914/transcript-

system. It has been publicly reported that nations such as Russia, China, Iran, and North Korea, as well as terrorist organizations and non-state actors, have attempted to and have the capability and intent to infiltrate our electrical systems, primarily through cyber-attacks.[3] There is also a growing awareness that we need to be concerned about the supply chain for software and equipment used in the electric industry.[4] The ability to remotely interfere with our electric system through cyber-attacks creates real threats to the physical operation of the grid. The Commission, NERC and regulated entities have been working to address these threats and must continue to do so.

4. Physical attacks on electric infrastructure are also a real threat. For example, the event that prompted Reliability Standard CIP-014-2 (Physical Security) was the April 2013 physical attack on the Metcalf substation in San Jose, California. This attack involved individuals using rifles to target the 500 kV substation; seventeen transformers were damaged in the attack.[5] Similarly, in September 2016, an individual armed with a high-powered rifle successfully conducted a sniper attack in Utah, knocking out the Buckskin substation and causing a loss of power for 13,000 customers.[6]

5. It is also recognized that remotely controlled unmanned aerial vehicles, or drones, can be employed to attack energy infrastructure. As an example, we only need to consider the public reports that drones were likely used to attack and damage oil refineries in Saudi Arabia in September, 2019.[7] We also need to be vigilant about the

---

dan-coats-warns-of-continuing-russian-cyberattacks.

[3] DEPARTMENT OF ENERGY, CYBER THREAT AND VULNERABILITY ANALYSIS OF THE U.S. ELECTRIC SECTOR at 20-23 (Aug. 2016), https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

[4] *See generally* Reliability Standard CIP-013-1, Cybersecurity – Supply Chain Risk Management.

[5] CONGRESSIONAL RESEARCH SERVICE, PHYSICAL SECURITY OF THE U.S. POWER GRID: HIGH-VOLTAGE TRANSFORMER SUBSTATIONS at 7 (Jun. 17, 2014), https://fas.org/sgp/crs/homesec/R43604.pdf.

[6] Peter Behr, *Substation attack is new evidence of grid vulnerability*, E&E NEWS (Oct. 6, 2016), https://www.eenews.net/stories/1060043920.

[7] David Reid, *Saudi Aramco reveals attack damage at oil production plants*, CNBC (Sep. 21, 2019), https://www.cnbc.com/2019/09/20/oil-drone-attack-damage-revealed-at-saudi-aramco-facility.html.

potential threat posed by various forms of electromagnetic pulse (EMP) when considering electric infrastructure security.[8]

President Executive Order

6. Among other actions taken by Congress and the President, on May 1, 2020, President Trump issued an Executive Order on "Securing the United States Bulk-Power System." In its preamble the Executive Order observes:

> [F]oreign adversaries are increasingly creating and exploiting vulnerabilities in the United States bulk-power system, which provides the electricity that supports our national defense, vital emergency services, critical infrastructure, economy, and way of life. The bulk-power system is a target of those seeking to commit malicious acts against the United States and its people, including malicious cyber activities, because a successful attack on our bulk-power system would present significant risks to our economy, human health and safety, and would render the United States less capable of acting in defense of itself and its allies.[9]

7. To address these threats, the Executive Order prohibits the purchase or use of equipment for the electric grid that was manufactured by an entity under the control of a foreign adversary or that poses a national security threat.

FERC and NERC Responses to Cyber and Physical Security

8. Under the Energy Policy Act of 2005, FERC, along with NERC, oversees implementation and enforcement of mandatory reliability standards for both cyber and physical security in the bulk electric system.[10] Through the development of Critical Infrastructure Protection or CIP standards, we ensure that the assets that support the nation's electricity supply comply with baseline standards for cyber and physical security. Though the Complaint at issue in this proceeding is denied, the work to secure the grid is ongoing.

---

[8] *See* Executive Order No. 13865, 84 Fed. Reg. 12041 (2019); *see also* DEPARTMENT OF ENERGY, ELECTROMAGNETIC PULSE RESILIENCE ACTION PLAN (January 10, 2017), https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf.

[9] *See* Executive Order No.13920, 85 Fed. Reg. 26595 (2020).

[10] Energy Policy Act of 2005, Pub. L. No. 109-58, § 1211, 119 Stat. 941-46 (2005) (codified at 16 U.S.C. § 824o).

9. The threats to the grid are real and we must remain vigilant. FERC and NERC have been working with industry to establish standards. But standards are only the beginning. In addition to these baseline standards, FERC and NERC must also work collaboratively with industry to establish best practices in addressing these threats. It is up to everyone to be vigilant and proactive in preventing attacks and mitigating security risks. As a Commission we need to work continually with NERC and the regulated community to ensure that our electric grid is secure against cyber and physical attacks.

For these reasons, I respectfully concur.

_____

Bernard L. McNamee
Commissioner