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 UNITED STATES DEPARTMENT OF ENERGY

I. INTRODUCTION

The Secretary of Energy, on behalf of the United States Department of Energy ("DOE" or "the Department"), files these comments in response to the Federal Energy Regulatory Commission ("FERC" or "Commission") and North American Electric Reliability Corporation ("NERC") Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards ("Joint White Paper") issued by FERC in Docket No. AD19-18-000.

As discussed herein, DOE generally supports the Joint White Paper's proposed revisions of the Notice of Penalty ("NOP") format for Critical Infrastructure Protection ("CIP") reliability standards. Protecting critical infrastructure from cyber and physical threats while transparently reporting reliability standard violations to FERC is a worthy but challenging task. DOE thus appreciates the attention that FERC and NERC staffs have given to proposing revisions of the NOP format for CIP reliability standards in their Joint White Paper, and recommends only slight adjustments in the approach.

Energy infrastructure is a primary target for hostile cyber actors, both state-sponsored and private. A number of well-documented attacks against critical infrastructure have already taken place in recent times, and DOE expects these attempts to continue. The 2019 National Intelligence Strategy, released by the Office of the Director of National Intelligence ("ODNI") in January 2019, supports this point. The Strategy notes that "[o]ur adversaries are becoming more adept at using cyberspace capabilities to threaten our interests and advance their own strategic and economic objectives."[1] ODNI also asserts that "[c]yber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices."[2] Additionally, ODNI asserts that two nation states already have the capability to execute cyber attacks against our critical infrastructure, including natural gas pipelines and the bulk power system.[3] With vigilance against cyber threats as a national priority, DOE shares the FERC and NERC staffs' intent "to protect sensitive information that could be useful to a person planning an attack on infrastructure while balancing the goals of transparency and efficiency."[4] More generally, DOE's focus is on recognizing the growing risks to the sector and appropriately protecting information so that the United States Government can assist in improving resilience and security and avoid creating vulnerabilities through inadvertent disclosures.

---

[1] Office of the Director of National Intelligence, *2019 National Intelligence Strategy of the United States of America*, at 11 (Jan. 22, 2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

[2] *Id.*

[3] *Id.*

[4] Joint White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards, FERC Docket No. AD19-18-000, at 4 (Aug. 27, 2019), https://www.ferc.gov/media/news-releases/2019/2019-3/AD19-18-000-Joint-White-Paper-NoFR.pdf.

This objective is also what is contemplated in the amendments to the Federal Power Act ("FPA") by the Energy Policy Act of 2005 and the Fixing America's Surface Transportation Act of 2015 ("FAST Act").[5] Section 215(e) of the FPA authorizes NERC, as the Commission-certified electric reliability organization, to impose a penalty on a user, owner, or operator of the Bulk-Power System for violation of a Commission-approved Reliability Standard.[6] In Order No. 672, the Commission stated that "the disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the Bulk-Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise."[7] The Commission explained that "a proceeding involving a Cybersecurity Incident requires additional protection because it is possible that Bulk-Power System security and reliability would be further jeopardized by the public dissemination of information involving incidents that compromise the cybersecurity system of a specific user, owner or operator of the Bulk-Power System,"[8] and that "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize system security, allowing persons seeking to do harm to focus on a particular entity in the Bulk-Power System."[9] On the other hand, in Section 215A of the FPA the Commission and the Secretary of Energy are given the authority to designate, protect, and share critical electric infrastructure information ("CEII"). The

[5] Section 61003 of the Fixing America's Surface Transportation Act of 2015, Pub. L. No. 114-94, 129 Stat. 1312, 1773-79 (2015), added section 215A to Part II of the Federal Power Act (codified at 16 U.S.C. § 824o-1), subsection (d) of which authorized both FERC and DOE to designate critical electric infrastructure information.

[6] 16 U.S.C. § 824o(e).

[7] 18 C.F.R. 39.7(b)(4); *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).

[8] Order No. 672, 114 FERC ¶ 61,104 at P 538.

[9] *Id.*

Department, similar to the Commission in its statements, supports an approach that provides maximum transparency unless the transparency unreasonably conflicts with security.

As described in greater detail below, in executing the intent of the revisions to the FPA and ensuring the resilience, reliability, and security of the nation's critical electric infrastructure, DOE recommends that FERC publicly disclose on a quarterly basis the number of violations of each CIP Reliability Standard violated broken down by the six NERC Regions. In addition, to help prevent inadvertent disclosure of information that could create vulnerabilities in the resilience and security of critical electric infrastructure, DOE recommends that FERC advise both NERC and regulated entities to add all appropriate FOIA exemption markings. Notably, the material may be both Confidential Business Information ("CBI") and CEII in light of the recent opinion of the Supreme Court of the United States in *Food Marketing Institute v. Argus Leader Media* (No. 18-481), which effectively broadens the scope of data and information that are eligible for the fourth exemption from disclosure under FOIA.

II. COMMENTS

A. FERC and NERC should only publicize on a quarterly basis the number of violations of each CIP Reliability Standard grouped by the six NERC Regions.

The Department recommends that FERC not publicize the names of CIP violators because the risk of security vulnerability outweighs the interest in transparency. The Department suggests that publicizing on a quarterly basis the number of violations of each CIP Reliability Standard, grouped by the six NERC Regions, is a middle-ground approach that would make the CIP NOP process as transparent as possible. This approach would allow for various statistical analysis to be conducted by the public without unreasonably compromising the security of the bulk-power system. For example, this information would allow interested parties to compare and analyze the performance between regions on particular CIP Reliability Standards and determine which NERC Regions have

the most violations of certain CIP Reliability Standards in order to recommend targeted mitigation help in those regions. The NERC Regional Entities could then provide the mitigation help to ensure compliance. In addition, it would allow a more thorough understanding of the enforcement of CIP Reliability Standards and the effectiveness of the enforcement regime by determining through several quarters whether particular CIP Reliability Standards were continually being violated or mitigation methods were working to improve performance.

The Joint White Paper outlines both the current and proposed practices. It states that "NERC's practice has been to request certain information in CIP NOPs, including the identity of the violator be designated as non-public and [Critical Electric Infrastructure Information ('CEII')] pursuant to the Commission's rules and regulations."[10] Further, the Commission maintains such "information . . . as non-public in [its] filing system . . . until such time as Commission staff determines that it is not entitled to CEII treatment (e.g., in response to a third-party information [request])."[11] Under the Joint White Paper's proposed format, NERC NOP submissions would be revised to include a "public cover letter that discloses the name of the violator" along with the standard(s) violated and the penalty amount, but would include other details as a non-public attachment and with a request for CEII designation. As written, the proposal allows NERC to name any violator for any violation and to release that information to the public.

Knowledge of a violator's identity, when combined with other available information, increases the bulk-power system's vulnerability (but to varying degrees depending on the type of violation). As the Joint White Paper highlights, "public identification of the CIP violator may result in increased hacker activity such as scanning of cyber systems and possible phishing

[10] Joint White Paper at 2.

[11] *Id.* at 2-3.

attempts."[12] The subsequent reassurance, however—"that the limited information provided in the proposed cover letter would not provide an adversary with insights on the nature of the CIP violation or related cyber vulnerabilities, processes or procedures that could be used for an informed, focused attack on the violator's cyber assets"—does not accurately describe the risk.[13] For example, if an aggressor knows who committed a violation, the aggressor can figure out who the entity's leaders are and launch a phishing campaign against them or attempt to scan the entity's cyber systems. Exposing violator identities therefore enables and helps to increase the success rate of additional threat vectors when linked to other available information. Additionally, exposing violator identities could disincentivize self-reporting above and beyond FERC and NERC requirements, to the detriment of threat information sharing (especially cyber) and complication of incident response for ongoing incidents under Presidential Policy Directive 41. Despite the consequences for transparency, withholding violator identities is the only reasonable way to avoid this undesirable result.

In comments on NOP dockets filed seven months ago, the trade groups American Public Power Association, Edison Electric Institute, and National Rural Electric Cooperative Association highlighted past FERC/NERC practice and explained the dangers of linking names to violations:

> [I]n 2010 NERC and the Commission intentionally chose to post only the public versions of the Notices of Penalty without the names of the entities to address security concerns because the names, when combined with information on the violations and penalties, were considered CEII. In addition to the entity names, details on cybersecurity vulnerabilities and mitigation measures that can be used by an attacker to determine which entity to target; what device or system to target; and how to target that entity, device, or system were also intentionally left out of the public versions. Disclosing this information to the public will not only be useful to those who seek to attack the bulk-power system, but will also have a

[12] Joint White Paper at 11.

[13] *Id.*

> negative impact on the effectiveness of the Commission's compliance and enforcement activity.[14]

The Department reaffirms this cautionary tale in its comments today, much as the Commission itself has guarded against it in its regulations at 18 C.F.R. 39.7(b)(4), where the identity of the violator is presumed nonpublic when the violation relates to a Cybersecurity Incident or could jeopardize bulk-power system security.

A wide range of aggressors could seek to take advantage of CIP violator information when security is at stake. For instance, hackers, certain foreign states, and other malicious actors, in addition to exposing vulnerabilities through phishing attacks, may probe and mine data and may post entity information on the Internet and dark web. Malicious actors may build scenarios to exploit vulnerabilities based on the quantity of violations, amounts of penalties, and standard areas. For instance, aggressors may attempt to use data to identify a utility that continually violates standards and concentrate their efforts on exploiting this weak link. Furthermore, an aggressor's basic data mining may reveal an entity's location, operating footprint, and maps of facilities for which the aggressor can make logical risk deductions based on penalty amounts. Hackers, certain foreign states, and other malicious actors can then attempt to use this information to concentrate their attacks. Using published data and basic data mining, they also may be able to link multiple entities' names and attack an entire region, causing even more severe risks to the bulk power system. For example, publicizing CIP-005 information violations for entities in a region may communicate that the region or group of entities at large have failed to manage firewalls, perimeters or interactive remote access, allowing inference of a weaker security posture for the

[14] Motion to Intervene and Protest of the American Public Power Association, the Edison Electric Institute, and the National Rural Electric Cooperative Association, at 14, United States of American Before the Federal Energy Regulatory Commission, (Docket No. NP10-130-000 et seq.) (Mar. 28, 2019).

region. Transparency is critical—fortunately, it is possible to maintain transparency without compromising security.

In the event the Commission adopts the Joint White Paper's proposal, the Commission should ensure that prior to releasing information including the name of the violators, the Commission fully analyze the data to ensure that hackers, certain foreign states, and other malicious actors cannot exploit it. If the Commission determines that such information may pose a security risk, as outlined above, such information should not be publicized.

B. FERC and NERC should routinely solicit Confidential Business Information markings from entities when they are submitting information in relation to CIP NOPs.

The Joint White Paper focuses on information in CIP NOPs being designated as CEII and exempt from release under FOIA exemption 3. However, the broader scope of FOIA exemption 4 is relevant in this case. The United States Supreme Court has recently expanded the range of material exempt from public disclosure under the Freedom of Information Act ("FOIA").[15] In its June 24, 2019 opinion in *Food Mktg. Inst. v. Argus Leader Media*, the Court held that "where commercial or financial information is both customarily and actually treated as private by its owner and provided to the government under an assurance of privacy, the information is 'confidential' within the meaning of [FOIA] Exemption 4."[16] CIP NOPs, as contemplated in the Joint White Paper, include such information, as do submissions from entities providing the pertinent details.

In light of the Supreme Court's opinion, FERC should advise NERC and registered entities submitting information to NERC related to CIP NOPs that particular material in their submissions

[15] 5 U.S.C. § 552(b)(4).

[16] *Food Mktg. Inst. v. Argus Leader Media*, No. 18-481, slip op. at 12 (U.S. June 24, 2019).

is marked as "Confidential Business Information," to identify the material likely to qualify for the FOIA exemption. To the extent registered entities believe information provided to NERC—and, in turn, to FERC—would be considered confidential business information, DOE recommends NERC inform registered entities mark all confidential business information to improve the overall protection of critical infrastructure information shared with the Government. DOE also suggests that NERC and FERC routinely solicit such "Confidential Business Information" markings when interacting with registered entities.

III. CONCLUSION

Protecting critical infrastructure from cyber threats while transparently reporting reliability standard violations to FERC is a worthy but challenging task. DOE thus appreciates the attention that FERC and NERC staffs have given to proposing revisions of the NOP format for CIP reliability standards in their Joint White Paper.

DOE appreciates the opportunity to submit comments in response to the Joint White Paper. As discussed above, we recommend that FERC publically disclose on a quarterly basis the number of violations of each CIP Reliability Standard violated according to the six NERC Regions without publicizing the names of CIP violators. In addition, DOE recommends that FERC and NERC advise registered entities submitting information related to CIP NOPs that particular material in

their submissions is marked as "Confidential Business Information," to identify the material likely to qualify for the FOIA exemption under the new legal standard set forth in opinion of the Supreme Court of the United States in *Food Marketing Institute v. Argus Leader Media* (No. 18-481).

Respectfully submitted,

/s Bruce J. Walker
Bruce J. Walker
Assistant Secretary
Office of Electricity
United States Department of Energy

/s Karen S. Evans
Karen S. Evans
Assistant Secretary
Office of Cybersecurity, Energy Security, and Emergency Response
United States Department of Energy

Dated: October 28, 2019

Document Content(s)