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 MISO TRANSMISSION OWNERS

Pursuant to the Federal Energy Regulatory Commission's ("Commission" or "FERC") August 27, 2019 Notice of White Paper and the Commission's September 19, 2019 Notice of Extension of Time, the MISO Transmission Owners[1] submit these comments in response to the August 27, 2019 Joint Staff White Paper on Notices of Penalty Pertaining to Violation of Infrastructure Protection Reliability Standards.[2] In the White Paper, Commission Staff and the

---

[1] The MISO Transmission Owners for this filing consist of: Ameren Services Company, as agent for Union Electric Company d/b/a Ameren Missouri, Ameren Illinois Company d/b/a Ameren Illinois and Ameren Transmission Company of Illinois; American Transmission Company LLC; Big Rivers Electric Corporation; Central Minnesota Municipal Power Agency; City Water, Light & Power (Springfield, IL); Cleco Power LLC; Cooperative Energy; Dairyland Power Cooperative; Duke Energy Business Services, LLC for Duke Energy Indiana, LLC; East Texas Electric Cooperative; Entergy Arkansas, LLC; Entergy Louisiana, LLC; Entergy Mississippi, LLC; Entergy New Orleans, LLC; Entergy Texas, Inc.; Great River Energy; Hoosier Energy Rural Electric Cooperative, Inc.; Indiana Municipal Power Agency; Indianapolis Power & Light Company; International Transmission Company d/b/a ITC*Transmission*; ITC Midwest LLC; Lafayette Utilities System; Michigan Electric Transmission Company, LLC; MidAmerican Energy Company; Minnesota Power (and its subsidiary Superior Water, L&P); Missouri River Energy Services; Montana-Dakota Utilities Co.; Northern Indiana Public Service Company LLC; Northern States Power Company, a Minnesota corporation, and Northern States Power Company, a Wisconsin corporation, subsidiaries of Xcel Energy Inc.; Northwestern Wisconsin Electric Company; Otter Tail Power Company; Prairie Power Inc.; Southern Illinois Power Cooperative; Southern Indiana Gas & Electric Company (d/b/a Vectren Energy Delivery of Indiana); Southern Minnesota Municipal Power Agency; Wabash Valley Power Association, Inc.; and Wolverine Power Supply Cooperative, Inc.

[2] Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards, Docket No. AD19-18-000 (Aug. 27, 2019) ("White Paper").

staff of the North American Electric Reliability Corporation ("NERC" and "NERC Staff," and with the Commission Staff, "Joint Staff") propose to change the current filing procedures used when NERC files a Notice of Penalty ("NOP") alleging a violation of a NERC Critical Infrastructure Protection ("CIP") Reliability Standard. Specifically, Joint Staff proposes to make public the name of the registered entity that is the subject to the NOP, the specific Reliability Standard that has been violated, and the amount of any penalty imposed.[3] While the proposed disclosure requirements could meet the perceived need of transparency, the White Paper does not articulate how Joint Staff's proposed disclosure requirements would benefit the reliability and security of the Bulk Electric System ("BES"). To the contrary, the proposed disclosure requirements could result in harm to the reliability and security of the BES. The White Paper also fails to demonstrate why additional transparency is needed. Accordingly, the changes proposed in the White Paper should not be adopted, and the Commission should retain its current policy of not publicly disclosing this information.

I. INTRODUCTION

A. Description of the White Paper and the Proposed Reforms

As described in the White Paper, a NOP submitted by NERC for an alleged violation of a CIP Reliability Standard typically includes the name of the alleged violator, nature of the violation, potential vulnerabilities to cyber systems as a result of the violation, and mitigation activities, with certain information, including the identity of the violator, designated as non-public and Critical Energy/Electric Infrastructure Information ("CEII").[4] Consistent with section 215A(d) of the

[3] *Id.* at 3, 8-9.

[4] *See id.* at 2, 8.

Federal Power Act ("FPA"), and section 388.113(d)(1)(iv) of the Commission's regulations,[5] the Commission's practice is to treat information asserted to be CEII as non-public information until such time as the Commission finds that the information is not entitled to CEII status.[6] Joint Staff claims that the Commission did not review NERC NOP filings for CEII status until, when it received, for the first time, a Freedom of Information Act ("FOIA")[7] request for the name of an undisclosed CIP violator.[8] Joint Staff states since then, the Commission has "received an unprecedented number" of FOIA requests for the release of non-public CIP NOP information.[9]

Joint Staff proposes to revise the NOP process so that NERC will submit CIP NOPs containing a public cover letter and confidential attachment, with the public cover letter disclosing the alleged violator's name, the Reliability Standard alleged to have been violated, and the penalty amount.[10] Additional information on the nature of the alleged violation, mitigation activities, and potential vulnerabilities to the cyber system would be provided in a confidential attachment for which CEII treatment could be requested.[11] Joint Staff states that NERC will submit a CIP NOP only after mitigation of the alleged violation has been completed, which Joint Staff claims will help minimize "the possibility of any adversarial insight resulting" from the public disclosures

---

5 16 U.S.C. § 824o-1(d); 18 C.F.R. § 388.113(d)(1)(iv).

6 White Paper at 2 (citing 18 C.F.R. § 388.113(d)(1)(iv)).

7 5 U.S.C. §552.

8 White Paper at 3.

9 *Id.* at 3.

10 *Id.* at 10.

11 *Id.* at 11.

contained in NOP filing.[12] This proposal would apply to "full" CIP NOPs, as well as to find, fix, and track filings and compliance exception reports.[13]

Joint Staff asserts that the proposed changes to the NOP procedures will have "multiple benefits," including providing a better security posture with respect to the public dissemination of potentially sensitive information, better adherence to the Commission's CEII regulations, and greater efficiency in the submission and processing of CIP NOPs.[14] Joint Staff acknowledges that the public disclosures of an alleged violator's name "may result in increased hacker activity," but claims the public disclosures contained in the cover letter would not provide sufficient information "for an informed, focused attack on the violator's cyber assets."[15] Joint Staff requests comment on the following subjects:

- The potential security benefits from the new proposed format;
- Any potential security concerns that could arise from the new format;
- Any other implementation difficulties or concerns that should be considered; and
- Does the proposed format provide sufficient transparency to the public.[16]

12 *Id.*

13 *Id.*

14 *Id.* at 9, 11-12.

15 *Id.* at 11.

16 *Id.* at 4, 12.

B. The MISO Transmission Owners

The MISO Transmission Owners are a group of investor-owned transmission owners, cooperatives, and municipal utilities that own transmission facilities over which the Midcontinent Independent System Operator, Inc. ("MISO") provides transmission service. The MISO Transmission Owners are subject to the NERC Reliability Standards, including certain of the NERC CIP Reliability Standards. To the extent a service list is established in the proceeding, the MISO Transmission Owners request that the Commission place the following individuals on such service list:

Wendy N. Reed
David S. Berman
WRIGHT & TALISMAN, P.C.
1200 G Street, N.W., Suite 600
Washington, DC 20005-3898
(202) 393-1200 (phone)
(202) 393-1240 (fax)
reed@wrightlaw.com
berman@wrightlaw.com

II. THE PROPOSED CHANGES WILL NOT ENHANCE OR BENEFIT SECURITY OR RELIABILITY AND SHOULD NOT BE ADOPTED

A. The Proposed Changes Offer Little If Anything in Terms of Potential Security Benefits

As described below, the proposed changes could pose significant harm to the reliability and security of the BES, and any nominal transparency benefits that they offer are not sufficient to offset this harm or the potential risks. While Joint Staff indicates that the primary benefit of the proposed changes in the NOP process would be increased transparency, Joint Staff fails to meaningfully balance the potential harms, or show that there would be any benefit to the owners or operators of the BES, and the assertion that the proposed changes would "more appropriately

balance[] confidentiality, transparency, security and efficiency concerns"[17] is unsupported. While Joint Staff claims the Commission has received an "unprecedented number of FOIA requests,"[18] Joint Staff fails to demonstrate that the existing procedures are not working or are overly burdensome, or to provide evidence of any harm or adverse results arising from the existing procedures.[19]

Additionally, some of the initial comments filed in response to the White Paper seem to presume or imply the public disclosure is necessary to ensure accountability or incentivize registered entities to be more diligent in complying with the CIP Reliability Standards.[20] Any such assertion is untrue. The MISO Transmission Owners are required to comply with CIP Reliability Standards, and operate their transmission systems in a safe, reliable and secure manner, dedicating financial, human, and operational resources towards such compliance. The MISO Transmission Owners also are audited and subject to sanctions if they fail to meet these requirements. Compliance with NERC Reliability Standards is an obligation that the MISO Transmission

---

17 *Id.* at 11.

18 *Id.* at 3.

19 Joint Staff also fails to quantify the number of FOIA requests FERC has received, or indicate whether these requests come from a broad array of interested parties, or from a small number of individuals. For example, one commenter in this proceeding has indicated that he has filed 235 FOIA requests. Comments and Alternative Proposal of Michael Mabee, Docket No. AD19-18-000, at 3 (Sept. 3, 2019) ("Mabee Comments"). While this may be a large part of the unprecedented number of FOIA requests the Commission has received, this does not mean that there is a significant public call for changing NERC's existing disclosure requirements.

20 *See* Mabee Comments at 6, 11; Comments on Transparency of Mary Kass, Docket No. AD19-18-000, at 1 (Sept. 24, 2019); Comments of Charles L. Manto as a Citizen, Docket No. AD19-18-000, at 2 (Sept. 20, 2019); Comments on Transparency of Dale D. Rowley, Docket No. AD19-18-000, at 1-2 (Sept. 15, 2019) ("Rowley Comments").

Owners take very seriously, and implication that they make any less of an effort to comply with these standards because their names would not be revealed in a NOP is incorrect.

Joint Staff also claims that disclosing the registered entity's name will lessen the chance its name will be inadvertently disclosed at a later date or that other sensitive information will be inadvertently disclosed.[21] However, Joint Staff fails to provide any evidence that this has been a significant issue in the past. If the concern is about inadvertent disclosure, the proper means to address this is through the development of proper controls and employee/contractor training, not through simply identifying the party that is the subject to the NOP. It is the act of identifying the registered entity's name that can increase the chance the entity will be subject to a cyber or physical security attack, not whether this disclosure is intentional or inadvertent.

Joint Staff claims that the proposed reforms are consistent with the "relevant law," including FPA section 215, the Fixing America's Surface Transportation Act, and FOIA.[22] However, both the FPA and the Commission's regulations allow for the protection of CEII, and provide that such information is exempt from disclosure under FOIA.[23] The Commission also has recognized that potential harm that can arise from the public disclosure of information involving cyber security events, stating:

> [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

---

21 White Paper at 12.

22 *Id.* at 4, 12 (citing FPA section 215, 16 U.S.C. §824o; Fixing America's Surface Transportation Act, Pub. L. No. 114-94, 129 Stat. 1312 (2015) ("FAST Act"); FOIA, 5 U.S.C. §552). The relevant sections of the FAST Act are codified at FPA section 215A, 16 U.S.C. § 824o-1(d).

23 *See* FPA section 215A(d), 16 U.S.C. § 824o-1(d); 18 C.F.R. § 388.113(c)(2); FOIA Exemptions 3 and 7(F), 5 U.S.C. §§ 552(b)(3) and 52(b)(7)(F); *see also* White Paper at 2 n.1.

> that compromise the cybersecurity system of a specific user, owner or operator of the Bulk-Power System. For example, 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. While the Commission recognizes the benefit of transparency in Commission proceedings . . . the benefits of transparency are overridden in the limited situation of cases in which such transparency would jeopardize Bulk-Power System security.[24]

Thus, the existing procedures are consistent with the relevant statutory and regulatory requirements.

B. Significant Security Concerns Could Arise from the New Format

While well-intentioned, the proposed disclosures and new format would increase the chance that a registered entity could be subject to cyber or physical security attacks. The White Paper fails to justify the increased security and reliability risk that would result. Joint Staff even admits that the additional disclosure may be a benefit to potential attackers.[25] The Commission should therefore decline to adopt the proposed reforms and NERC should continue to file NOPs requesting CEII treatment without revealing the name of the registered entity that is the subject of the NOP.

Disclosing the registered entity's name, the Reliability Standard alleged to have been violated, and the underlying fine, will provide bad actors – the parties likely to engage in cyber or

---

[24] *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 at P 538 (footnote omitted), *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006); *see also Revision to Electric Reliability Organization Definition of Bulk Electric System*, Order No. 743, 133 FERC ¶ 61,150, at P 2 (2010) (stating Congressional intent in enacting FPA section 215 was to "protect reliability of the nation's Bulk-Power System"), *order on reh'g*, Order No. 743-A, 134 FERC ¶ 61,210 (2011).

[25] *See* White Paper at 11 (conceding that "[t]he public identification of the CIP violator may result in increased hacker activity such as scanning of cyber systems").

physical security attacks – with information that can reveal weaknesses in a registered entity's cyber and physical security defenses. For example, if it is publicly disclosed that a transmission owner had one or more violations of Reliability Standard CIP-007 Reliability Standard (Cyber Security — System Security Management), this would let an attacker know that this specific transmission owner has issues with patching its systems. Moreover, even this limited information identifying the transmission owner could lead an attacker to a potential weak spot of that specific transmission owner. Similarly, an indication of a violation of Reliability Standard CIP-006-6 (Cyber-Security – Physical Security of BES Cyber Systems) or Reliability Standard CIP-014-2 (Physical Security) would indicate a weakness in the physical security of BES Cyber Systems or at the transmission owner's substations and control centers, similarly pointing an attacker to a potential weak spot. Moreover, if the NOP includes the name, Reliability Standard violated, and dollar amount of violations on a cover sheet for each filed NOP, a bad actor will be able to easily take that information to the NERC website, and by reviewing the CIP Reliability Standards and the Violation Risk Factors and the Violation Severity Level Matrixes, get a much better idea as to the nature of the violation and what systems or assets were affected than is publicly disclosed in the NOP. Unless NERC changes its current policies regarding what NOP information is posted on its website, which the White Paper does not address, the proposed new NOP format will enable bad actors to have more readily accessible information, enhancing their ability to negatively impact the BES.

Knowing the size of a fine could give some insight to how serious an alleged CIP violation was. Violation severity levels are clearly defined in NERC's CIP Reliability Standards for low, medium, and high BES Cyber Systems. The combination of knowing the size of the fine, the

company name, and knowledge of that CIP Reliability Standard, could also give a potential attacker a means to figure out the criticality of BES Cyber Systems an entity may possess.

Additionally, the sharing of threat intelligence and lessons learned are practices that the utility industry is embracing. This should be encouraged, with the ultimate goal of increasing the safety, reliability, and security of the grid. Public disclosure of NOP information could inhibit sharing of threat intelligence and lessons learned. For example, if implemented, this proposal could erode confidence that information that is voluntarily shared would not be disclosed to outside parties. Moreover, while companies are willing to share lessons learned because they know there is some protection in the fact that they can remain anonymous to the public, sharing this type of information often provides greater detail about why an event occurred. Without the protection of anonymity, this type of information could provide roadmaps to bad actors.

Moreover, providing identifying information in a public forum may disproportionately impact smaller, less security-capable, registered entity. For example, presume that both registered entity A (a large utility) and registered entity B (smaller utility) were both subject to NOPs and the public disclosure of their names. This could lead attackers to speculate that the latter – being smaller and therefore potentially less defensively capable – might require less effort to attack than the former. While such presumption by a bad actor might not be accurate, the effect is that registered entity B could be at greater risk of being attacked.

Further, Joint Staff indicates that delaying the filing of the NOP until mitigation is complete will address concerns that could arise from publicly disclosing the name of a registered entity that has been subject to cyber or physical system attack.[26] Even if the mitigation is complete, public disclosure of a registered entity's name, especially combined with the CIP Reliability Standards

[26] *Id.* at 11.

violated and the size of the fine, could make the registered entity subject to increased attacks if it is perceived as vulnerable or as a good target. Moreover, the Commission should recognize the BES functions as an integrated system. While the reform proposed in the White Paper would involve the name of the registered entity that is the subject of the NOP, any actions that encourage attacks on that entity could impact the BES as a whole. NERC should continue to file NOPs requesting CEII treatment without revealing the name of the registered entity that is the subject of the NOP.

If the Commission determines that some additional level of transparency is needed, it should consider more limited measures than set forth in the White Paper, such as releasing the name of the registered entity for certain violations and an indicator of the seriousness of the violation, without disclosing the specific Reliability Standard that has been violated. For example, for certain violations, the United States Nuclear Regulatory Commission releases the name of the violator and a color-code of green, white, yellow, or red based on the risk significance.[27] The Commission should consider a similar approach, and also consider disclosing a bandwidth of penalty amounts, rather than disclosing the specific amount assessed.

Additionally, if the Commission adopts reforms to allow public disclosure of a registered entity's name, the Commission should only allow for the public disclosure of low impact violations to lessen the value to bad actors of the information disclosed, and protect more critical assets and

[27] *See Enforcement Process Diagram*, United States Nuclear Regulatory Commission, https://www.nrc.gov/about-nrc/regulatory/enforcement/enforce-pro.html (last visited Oct. 28, 2019); *Nuclear Regulatory Commission Enforcement Manual*, United States Nuclear Regulatory Commission, sections 1.1.1 & 1.1.2 (Rev. 10, Change 4, Aug. 16, 2019), https://www.nrc.gov/docs/ML1920/ML19207A161.pdf.

functions. The Commission also should make it clear that the name of an alleged CIP Reliability Standard violator can be redacted for good cause shown.[28]

In addition, the proposal to make this information publicly available for compliance exceptions[29] is unnecessary. Compliance exceptions are non-substantive and minimal risk.

C. No Additional Transparency Is Needed

Joint Staff asks whether the proposed reforms provide sufficient transparency to the public.[30] While Joint Staff does not indicate what additional reforms it has in mind, a number of commenters urge that the Commission impose even broader public disclosure requirements.[31] The MISO Transmission Owners strongly oppose any further extension of proposed public requirements that reveal other CEII or confidential information, such as details about the alleged violations or any attack, the specific systems affected, the extent of any damage, and specific mitigation measures adopted. The more information that is released, the greater the risk to cyber security, specific entity assets, and reliability, as releasing more information will make it easier for bad actors to search for vulnerabilities and attack the BES. This entire premise (releasing information) seems contrary to the CIP Reliability Standards, which are intended to increase security and implement requirements to protect cyber assets. NERC and the Commission should retain their current policy of not publicly disclosing the name of a registered entity subject to a NOP, and should not take any steps that expand the scope of the information released.

---

28 White Paper at 11 (Joint Staff acknowledges that this is appropriate).

29 *See id.*

30 *Id.* at 12.

31 *See* Mabee Comments at 4-11; Rowley Comments at 1-2; Comments on Transparency of Ken Sletten, Docket No. AD19-18-000, at 2 (Sept. 23, 2019).

III. CONCLUSION

For the reasons stated above, the Commission should take these comments into consideration and decline to require the changes proposed in the White Paper.

Respectfully submitted,

/s/ David S. Berman
Wendy N. Reed
David S. Berman
WRIGHT & TALISMAN, P.C.
1200 G Street, N.W., Suite 600
Washington, DC 20005-3898
(202) 393-1200 (phone)
(202) 393-1240 (fax)
reed@wrightlaw.com
berman@wrightlaw.com

Attorneys for
The MISO Transmission Owners

October 28, 2019

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document upon each person designated on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, DC, this 28th day of October 2019.

/s/ David S. Berman
David S. Berman
WRIGHT & TALISMAN, P.C.
1200 G Street, N.W., Suite 600
Washington, DC 20005-3898

Attorney for the
MISO Transmission Owners

Document Content(s)