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 WOLVERINE POWER SUPPLY COOPERATIVE, INC.

Wolverine Power Supply Cooperative, Inc. ("Wolverine") welcomes the opportunity to submit its comments in response to the joint White Paper (the "White Paper") prepared by the staffs of the Federal Energy Regulatory Commission (the "Commission") and the North American Electric Reliability Corporation ("NERC").[1] As described more fully below, Wolverine is opposed to the White Paper's proposal to publicly release the name of an entity that is the subject of a Notice of Penalty ("NOP") for a violation of Critical Infrastructure Protection ("CIP") Reliability Standards. While releasing the name of the entity responsible for a violation may increase transparency and provide other potential benefits, these perceived improvements are outweighed by security concerns. When a responsible party's name is combined with other publicly available information about a violation, a bad actor (a person planning an attack on critical electric infrastructure) is granted a "road map" to target known vulnerabilities in the Bulk-Power System. This jeopardizes the safety of the Bulk-Power System—the opposite effect intended by the Commission.

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

I. BACKGROUND

A. The White Paper and this Comment Docket

The White Paper addresses NERC's submission, and the Commission's processing, of NOPs for violations of CIP Reliability Standards. The CIP Reliability Standards contain requirements that provide for the cybersecurity of the Bulk-Power System. The CIP NOPs that NERC submits to the Commission typically include information about the nature of the violation, potential vulnerabilities to cyber systems caused by the violation, and related mitigation activities. NERC's practice has been to request certain information included in CIP NOPs, including the identity of the violator, be designated as nonpublic and Critical Energy/Electric Infrastructure Information ("CEII") pursuant to Commission regulations.[2] This CEII designation for certain sensitive information is intended to protect the security of the Bulk-Power System.

The Commission's practice is to treat information received under a CEII designation as nonpublic until such time as Commission staff determines that the information is not entitled to CEII treatment (for example, in response to a third-party Freedom of Information Act ["FOIA"] request). According to the White Paper, NERC has submitted CIP NOPs containing CEII requests since 2010, but did not receive a FOIA request seeking the name of an undisclosed CIP violator (which NERC refers to as an "unidentified registered entity" or "URE") until eight years later, in 2018.[3] Recently, the Commission received an "unprecedented number of FOIA requests" seeking nonpublic information in CIP NOPs, including the identity of UREs.[4] This prompted Commission and NERC staff to reevaluate the CIP NOP process and led to the issuance of the White Paper and

[2] *See* 18 C.F.R. § 388.113 (2018); 18 CFR § 39.7(b)(4) (2018).
[3] White Paper at 3.
[4] *Id.*

the request for comments thereon, which proposes a revised CIP NOP format intended to achieve a more appropriate balance between security and transparency.

Specifically, the proposal described in the White Paper would require NERC to submit CIP NOPs with a public cover letter. This public cover letter would disclose the name of the violator, the CIP Reliability Standard(s) violated, and the penalty amount. The remainder of the CIP NOP filing details (including the nature of the violation, mitigation activity, and potential vulnerabilities to cyber systems) would be submitted as a nonpublic attachment, and would continue to be accompanied by a request for the designation of the information as CEII.[5]

B. Wolverine

Wolverine is a Michigan-based, not-for-profit generation and transmission electric cooperative that provides wholesale service to its seven members and is subject to the Commission's jurisdiction under the Federal Power Act. Wolverine generates and purchases electricity primarily to serve its members-owners and supplements and balances its power supply portfolio with short-term purchases from, and sales to, the Midcontinent Independent System Operator, Inc. ("MISO") and PJM Interconnection, L.L.C. markets. Wolverine is a Transmission-Owner member of the MISO with a transmission system consisting of approximately 1,600 miles of 69 kV and 138 kV looped transmission lines and associated facilities. Wolverine's transmission facilities are subject to the terms of the MISO Open Access Transmission, Energy and Operating Reserve Markets Tariff ("MISO Tariff") and are located in the Michigan Joint Zone pursuant to Attachment O of the MISO Tariff.

[5] *Id.* at 10-11.

II. COMMUNICATIONS

All correspondence and pleadings relating to this proceeding should be addressed to the following individuals:

Tom King Jr.*
Director of Regulation and Policy
Wolverine Power Supply Cooperative, Inc.
10125 W. Watergate Road
Cadillac, MI 49601
Tel: (231) 779-3325
tking@wpsci.com

Michael J. Rustum*
Halima A. Nguyen
Winston & Strawn LLP
1700 K Street, N.W.
Washington, DC 20006-3817
Tel: (202) 282-5645
mrustum@winston.com
hanguyen@winston.com

*designated for service.

III. COMMENTS

While Wolverine supports greater compliance, transparency, and reliability of the Bulk-Power System, Wolverine is opposed to the White Paper proposal to publicly release the name of an entity that is the subject of a CIP NOP. As the Commission noted in its rulemaking proceeding establishing the original CIP NOP procedures, releasing the name of an entity that has violated a CIP Reliability Standard and is potentially vulnerable to a cyber-attack, places the safety of the Bulk-Power System at risk. It is unclear what changed in the past decade—beyond increasing administrative inconvenience—to lead the Commission to change its position and now conclude otherwise. If the Commission and NERC wish to increase transparency by releasing additional information about CIP NOPs, Wolverine proposes that the CIP NOP disclose the region of the entity on the public cover sheet rather than the specific entity name. If the Commission's goal is to deter violations, Wolverine proposes that other punitive measures may be instituted instead, such as increasing the monetary penalties imposed on violators and/or implementing additional compliance oversight.

A. Disclosing the Name of an Entity Jeopardizes the Safety of the Bulk-Power System

As part of the CIP NOP process, a large amount of information about CIP Reliability Standard violations is released to the public. For example, the NERC website includes a publicly available "Searchable NOP Spreadsheet," which includes information such as the Reliability Standard(s) and particular Requirement(s) violated and the risk level presented by the violation.[6] Releasing the name of the entity that is the subject of the NOP, in addition to the other information available, presents a potential attacker with a "road map" to identify weaknesses in critical electric infrastructure to exploit through a targeted attack. Publicly identifying the entity and/or the vulnerable standard will enable an attacker to expose and target a single point of weakness in the Bulk-Power System, and would leave the entity vulnerable to attacks intended to exploit this publicly identified vulnerability.

The Commission recognized the risk presented by disclosing the name of an entity during the rulemaking process through which it established the original CIP NOP regulations. In Order No. 672,[7] in which the Commission promulgated regulations to address NERC's development and enforcement of Reliability Standards, the Commission emphasized the risks inherent in revealing the name of an entity with a cybersecurity vulnerability:

> As explained in the NOPR, and confirmed by numerous commenters, 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. 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

[6] *See* Searchable NOP Spreadsheet, NERC, Enforcement and Mitigation, https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx (last accessed Sept. 13, 2019).
[7] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

> Commission proceedings . . . the benefits of transparency are overridden in the limited situation of cases in which such transparency would jeopardize Bulk-Power System security. . . . [I]n balance, Commission authority to establish a nonpublic proceeding if necessary and lawful, including but not limited to, a proceeding involving a Cybersecurity Incident, serves an important public interest that outweighs the competing goals of openness and transparency.[8]

The White Paper noted this concern, but emphasized that the provisions of the regulations related to maintaining information and proceedings as nonpublic "pertain to limited situations involving a Cybersecurity Incident or other matters that would jeopardize Bulk-Power System security if publicly disclosed."[9] However, as quoted above, the Commission previously recognized that the public interest of maintaining the safety and security of the Bulk-Power System "outweighs the competing goals of openness and transparency," in circumstances "*including but not limited to*, a proceeding involving a Cybersecurity Incident."[10]

Consistent with this determination, Commission and NERC procedures have maintained the identity of an entity that is the subject of a CIP NOP as nonpublic and CEII for the past decade. Disclosing the name of the entity that has violated a CIP Reliability Standard, when combined with other publicly available information, jeopardizes the security of the Bulk-Power System. This disclosure sacrifices public safety in favor of increased transparency, but the increase in risk outweighs any benefit that could be gained by releasing the name of the entity.

Furthermore, as former Commissioner LaFleur noted in her statement released concurrently with the White Paper, the procedures that NERC and the Commission have followed in processing CIP NOPs have not changed in the past decade.[11] The White Paper does not indicate what, if anything, has changed in the thirteen years since Order No. 672 was released that would

[8] Order No. 672 at P. 538-39 (emphasis added) (citations omitted).
[9] White Paper at 6.
[10] Order No. 672 at P. 539 (emphasis added).
[11] *White Paper Docket*, Statement of Commissioner LaFleur, Docket No. AD19-18-000 (filed Aug. 27, 2019).

lead the Commission to invalidate its earlier finding that "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize system security." There is nothing in the White Paper to support this sudden reversal in findings or support the new conclusion that releasing the name of an entity subject to a CIP NOP would no longer endanger the Bulk-Power System. While determining, on a case-by-case basis, whether publicly identifying an entity presents a security risk may be an administrative inconvenience, the inconvenience is, unfortunately, necessary to remain vigilant in the face of increasingly sophisticated efforts to exploit system vulnerabilities, including through cyber-attack. Accordingly, Wolverine urges the Commission and NERC to maintain the procedure of protecting the entity name as CEII, consistent with longstanding practice, to protect the safety of the Bulk-Power System.

B. The Commission Should Seek Alternate Proposals to Both Achieve Its Goals and Protect the Security of the Bulk-Power-System

The White Paper indicates that the Commission and NERC are seeking ways to "appropriately balance[] security and transparency concerns."[12] Wolverine supports the goals of transparency and deterring violations of the CIP Reliability Standards. However, there are ways to increase transparency and deter violations without disclosing the name of vulnerable entities and providing attackers a "road map" to target known weaknesses in the Bulk-Power System. Wolverine urges the Commission to seek alternate proposals to achieve these goals that will present less danger to the security of the nation's electric infrastructure.

i. The CIP NOP cover page could identify the region, not the entity name

One possible way to increase transparency while reducing the resulting threat to the Bulk-Power System would be to release the entity's region for compliance—for example, the Reliability*First* ("RF") region—as opposed to the entity's name on the public cover sheet for CIP

[12] White Paper at 4.

NOPs. This compromise would provide the public with more information and allow for statistical analyses of the power system and CIP violations without opening individual entities to the risk of attacks targeted at now-known infrastructure weaknesses.

ii. The Commission should deter violations through means other than releasing the entity's name

Releasing the name of an entity could help to deter further violations because of the bad publicity that accompanies an announcement of a violation. However, as described above, the release of an entity's name presents significant risks to the security of the Bulk-Power System. If the Commission and NERC seek to deter further violations while still protecting vulnerable entities from the risk of targeted attacks, Wolverine urges alternative solutions such as increasing monetary penalties and/or implementing additional compliance oversight. Such a solution would deter further violations and encourage an entity to quickly mitigate the violations while still protecting the safety of electric infrastructure.

IV. CONCLUSION

For the reasons outlined above, Wolverine urges the Commission to continue to protect the name of an entity that violated a CIP Reliability Standard as CEII. Wolverine appreciates the opportunity to provide the Commission and NERC Staffs with its perspective on the foregoing matters.

Respectfully submitted,

/s/ Michael J. Rustum

Michael J. Rustum
Halima A. Nguyen
Winston & Strawn LLP
1700 K Street, NW
Washington, DC 20006
Tel: (202) 282-5645
Email: mrustum@winston.com
hanguyen@winston.com

Counsel for Wolverine Power Supply Cooperative, Inc.

Dated: October 15, 2019

Document Content(s)