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 ISO-RTO COUNCIL

Pursuant to the Federal Energy Regulatory Commission's (the "Commission" or "FERC") Notice of White Paper issued on August 27, 2019,[1] and Notice for Extension of Time issued on September 19, 2019,[2] the ISO-RTO Council ("IRC")[3] respectfully submits these comments in response to the White Paper in which FERC staff and staff of the North American Electric Reliability Corporation ("NERC")[4] propose a new format for NERC's

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

[2] *Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards*, Notice of Extension of Time, Docket No. AD19-18-000 (Sept. 19, 2019).

[3] The IRC comprises the following independent system operators ("ISOs") and regional transmission organization ("RTOs"): Alberta Electric System Operator ("AESO"), California Independent System Operator ("CAISO"), Electric Reliability Council of Texas, Inc. ("ERCOT"), the Independent Electricity System Operator of Ontario, Inc. ("IESO"), ISO New England, Inc. ("ISO-NE"), Midcontinent Independent System Operator, Inc. ("MISO"), New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection, L.L.C. ("PJM"), and Southwest Power Pool, Inc. ("SPP"). AESO and IESO are not subject to the FERC's jurisdiction and therefore do not join this filing.

[4] *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").

submission of Notices of Penalty[5] involving violations of NERC Critical Infrastructure Protection ("CIP") Reliability Standards.[6]

I. COMMENTS

The IRC supports the FERC and NERC staffs' goal of ensuring there is a sufficient balance between security and transparency. As described further below, the IRC believes an appropriate balance between these objectives may be achieved with the following modifications to joint staffs' proposed format for submitting Notices of Penalty:

1. The public cover letter for a Notice of Penalty should not specify which Reliability Standards were violated.

2. Find, fix, and track and compliance exceptions should be exempt from the proposal.

3. The identity of a Registered Entity[7] should not be disclosed in a Notice of Penalty until all appeals at NERC and FERC are exhausted.

4. Each Registered Entity associated with a Notice of Penalty should be permitted to request that NERC withhold disclosure of its name and to request Critical Energy and Electric Infrastructure Information ("CEII") treatment of the same for unique facts and circumstances that would cause a significant threat to either that company's or the industry's overall exposure to cyber-attacks.

---

[5] "'Notice of Penalty' means a notice prepared by NERC and filed with FERC, following approval by NERC of a Notice or other notification of Confirmed Violation or a settlement agreement, stating the Penalty or sanction imposed or agreed to for the Confirmed Violation or as part of the settlement." *Rules of Procedure of the North American Electric Reliability Corporation* ("NERC Rules of Procedure"), Appendix 2, Definitions Used in the Rules of Procedure, Definition of Notice of Penalty.

[6] "'Reliability Standard' means a requirement, approved by the United States Federal Energy Regulatory Commission under Section 215 of the Federal Power Act, or approved or recognized by an applicable governmental authority in other jurisdictions, to provide for Reliable Operation of the Bulk Power System. The term includes requirements for the operation of existing Bulk-Power System facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for Reliable Operation of the Bulk-Power System, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity…." NERC Rules of Procedures, Appendix 2, Definitions Used in the Rules of Procedure, Definition of Reliability Standard.

[7] "'Registered Entity' means an owner, operator, or user of the Bulk Power System, or the entity registered as its designee for the purpose of compliance, that is included in the NERC Compliance Registry." NERC Rules of Procedures, Appendix 2, Definitions Used in the Rules of Procedure, Definition of Registered Entity.

5. Each Registered Entity should be provided notice and an opportunity to comment on Freedom of Information Act ("FOIA")[8] requests pertaining to its notices of penalties.

6. Joint staffs should clarify that NERC will continue to follow the Commission's CEII submission procedures to ensure that CEII status and the associated protections are properly invoked.

7. NERC should revise its Rules of Procedure to conform with the White Paper.

8. NERC, the Commission, and stakeholders should explicitly identify alternative means for sharing the information that will become unavailable as a result of any Notice of Penalty revisions ultimately adopted.

Moreover, as explained below, the IRC believes that the issues in this proceeding also implicate the Commission's broader administration of its regulations relative to the release of CEII. The IRC urges the Commission to undertake a review of those practices to ensure they appropriately protect critical security information. With this backdrop in mind, the IRC provides the following in response to the specific comments requested by joint staffs.

A. The Potential Security Benefits from the New Proposed Format

The IRC appreciates the potential security concerns raised by joint staffs associated with the current practice of redacting Notices of Penalty on a line-by-line basis. As stated in the White Paper, this process introduces many opportunities for error, such as the inadvertent disclosure of critical security information. Moreover, there is a risk that malicious actors could deduce information that could jeopardize the security of the bulk-power system from seemingly insignificant details in the redacted version of the Notice of Penalty. Joint staffs' proposal to include the details of the violation, mitigation activity, and potential vulnerabilities to cyber systems as a non-public attachment in each Notice of

[8] 5 U.S.C. §§ 552, *as amended* by the FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 (2016).

Penalty filed with FERC, along with a request for the designation of such information as CEII, may mitigate some of those risks. However, joint staffs' proposal also introduces some new risks that merit revisions to its proposal, as described herein. Additionally, the IRC also urges FERC to consider whether revisions to the administration of its CEII regulations are necessary to prevent inappropriate disclosure of CEII under any submission process.

B. The IRC's Security Concerns with, and Proposed Revisions to, the Commission and NERC's Proposed Notice of Penalty Format

As the joint staffs recognize in the White Paper, "[t]he public identification of a CIP violator may cause increased hacker activity such as scanning of cyber systems and possible phishing attempts."[9] The IRC agrees. The IRC believes, however, that joint staffs' proposed approach would increase the likelihood that malicious actors could identify and target a Registered Entity's problem areas and other vulnerabilities pertaining to cyber security because it would generally require disclosure of the Reliability Standard that was violated. As the Commission previously recognized, information related to CIP violations and cyber security issues, including the identity of the Registered Entity, may jeopardize bulk power system security because "…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."[10] The White Paper underestimates the security risks of publicly identifying *both* the

[9] White Paper at 11.

[10] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, Order No. 672, 2006-2007 FERC Stats. & Regs., Regs. Preambles ¶ 31,204, at P 538, *order on reh'g*, Order No. 672-A, 2006-2007 FERC Stats. & Regs., Regs. Preambles ¶ 31,212 (2006).

Registered Entity along with the Reliability Standards the Registered Entity violated and provides little justification for the increased security risks other than general benefit of increasing transparency and efficiency.

Moreover, the joint staffs' proposal could inadvertently deter self-reports of potential violations of Reliability Standards that are typically submitted out of an abundance of caution. Rules and practices should serve to encourage such self-reporting. Anonymity encourages self-reporting of such borderline violations. A Registered Entity that would ordinarily self-report such violations may be reluctant to do so if it increases the likelihood that a malicious actor could identify weaknesses or systematic failures by the Registered Entity to comply with a particular Reliability Standard, which increased risk of harm the Commission has acknowledged could occur by publicly identifying a Registered Entity and its associated CIP violation.[11]

For example, publicly identifying that a specific Registered Entity consistently violates CIP-010 (*Configuration Change Management and Vulnerability Assessments*) is akin to publicly identifying that the Registered Entity consistently has issues preventing and detecting unauthorized changes to its cyber systems, which is information that would be very useful to a hacker trying to infiltrate the Registered Entity's cyber systems. This may deter the Registered Entity from self-reporting, and the associated benefits of doing so—such as industry communication, lessons learned, and sharing of best practices—would be lost.

[11] *See id.* ("…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.) (citations omitted).

The IRC does not raise these concerns to argue that *no* information concerning the name or nature of the violation should be publicly released. Rather, the IRC proposes a balanced approach to address these concerns in light of joint staffs' interest in providing as much transparency as is reasonable under the circumstances.

C. IRC's Suggested Approach

To reduce the negative effects of the proposed new format, the IRC suggests several revisions to joint staffs' proposal.

1. Violated CIP Reliability Standards Should not be Specified in NERC's Cover Letter

In the White Paper, the joint staffs propose a Notice of Penalty format that would disclose the CIP Reliability Standards violated but would not disclose the requirements under those Reliability Standards.[12] Other than achieving the general outcome of making more information publicly known, joint staffs failed to articulate a reason or benefit for publicly disclosing the Reliability Standard violated. Moreover, the joint staffs' proposed Notice of Penalty format and White Paper imply that knowledge of the violated Reliability Standard is less sensitive than other information in the Notice of Penalty and, therefore, can be publicly disclosed with little to no consequences for security. However, even this high-level information—as discussed above in section I (B)—could provide some indication of vulnerabilities to target and is of little foreseeable public benefit. Therefore, the IRC proposes that the revised Notice of Penalty format not identify or enumerate the specific Reliability Standards violated.

[12] White Paper at 3.

As an alternative to the proposal in the White Paper, the proposed public cover letter that NERC would submit to FERC could include only the name of the violator, the amount of the penalty, and more generic violation information such as the number of violations or number of Reliability Standards violated, but not the specific Reliability Standards violated. For example, the cover letter could generally include the identity of the Registered Entity, number of Reliability Standards violated, number of violations, and penalty amount, without identifying the names of the Reliability Standards violated (e.g., "Registered Entity ABC committed ten violations over four standards resulting in a penalty amount of X dollars"). This would still provide the public transparency and associated accountability benefits from publicly identifying that the Registered Entity violated Reliability Standards, thereby providing states, shareholders and stakeholders who, in various ways, oversee the management of the organization with some indication of how the Registered Entity is faring in addressing security risks relative to its peers.

2. Joint Staffs Should Exempt From its Proposal Find, Fix, And Track and Compliance Exceptions

The IRC proposes that find, fix, and track and compliance exceptions be exempted from the White Paper proposal and continue to remain under seal. Many Reliability Standard violations result in find, fix, and track and compliance exceptions and are identified via self-reports. Many of those self-reported violations are borderline violations that are arguably not violations of Reliability Standards, but are submitted out of an abundance of caution, and result in no further action by NERC or FERC. There is little benefit associated with publicly releasing find, fix, and track penalties and compliance exceptions. Nevertheless, as discussed above in section I (B), releasing this seemingly innocuous information could be used by malicious parties to identify vulnerabilities in the

Registered Entity's systems. This, in turn, could deter self-reporting under the conditions noted. Excluding find, fix, and track and compliance exceptions would: (1) help mitigate these security risks by continuing to maintain critical security information as non-public; and (2) continue to ensure the anonymity needed to encourage self-reporting of potential violations, many of which are submitted out of an abundance of caution.

Although the IRC is cognizant of Commission precedent calling for the public release of information on find, fix and track penalties, that precedent need not automatically control in this process.[13] The issue in that previous proceeding was whether find, fix and track should be immune from any public disclosure. In the current proceeding, the joint staffs' proposal in the White Paper creates a new process that increases the level of transparency beyond what was before the Commission in the previous proceeding. Although the IRC believes that the experience gained justifies revisiting that precedent, nothing in the Commission's order in the previous proceeding is directly applicable or would allow staff to extend that precedent to issues that were simply not before the Commission at the time that order was issued.

3. The Identity of a Registered Entity in a Notice of Penalty Should not be Disclosed Until all Appeals at NERC and FERC are Exhausted

The IRC supports the Commission's proposal that NERC only submit the Notices of Penalty after the mitigation activities are complete. Moreover, the IRC suggests that the identity of a Registered Entity in a Notice of Penalty not be disclosed until all appeals at

[13] *North American Electric Reliability Corporation*, Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing, Docket Nos. RC11-6-000, et al. (Mar. 15, 2012).

NERC and FERC are exhausted to ensure that only confirmed, non-appealable violations are being reported.

4. Each Registered Entity Associated with a Notice of Penalty Should be Permitted to Request that NERC Withhold Disclosure of its Name in a Public Filing and to Request CEII Treatment of the Same

While the IRC agrees with the proposal in the White Paper that NERC should, in appropriate circumstances, be permitted to withhold disclosure of an entity's name in the public filing and to request CEII treatment, the IRC suggests that a similar process be permitted for the Registered Entities.[14] This safety-valve process would allow a Registered Entity to argue to NERC and FERC that disclosure of the identity of the Registered Entity or violation could, based on unique facts and circumstances, cause a significant threat to either that company's or the industry's overall exposure to cyber-attack. Under this approach, mere reputational damage would not suffice to meet this test; however, a showing that disclosure of the information in the public cover letter could exacerbate specific exposure would be sufficient for invoking this exception to disclosure. The process should include set deadlines to allow the Commission to act quickly in response to the public's request, while still providing time for the Registered Entity to seek such relief and the Commission to timely consider the unique facts and circumstances of each case.

5. Each Registered Entity Should be Provided Notice and an Opportunity to Comment on FOIA Requests Pertaining to its Notices of Penalties

Consistent with FERC's current approach for FOIA requests pertaining to CIP Notices of Penalty, the Commission and NERC should continue to provide each Registered

[14] White Paper at 11.

Entity notice of any FOIA request for the information in a Notice of Penalty and an opportunity to comment on the CEII status of the information. Registered Entities will be able to provide facts and a perspective that are unavailable to FERC and could assist the Commission with its determination of whether to grant the FOIA request. Moreover, this process and the associated deadlines should be codified in the NERC Rules of Procedure and the Commission's rules and regulations.

6. The White Paper Should Clarify that NERC Will Continue to Follow the Commission's CEII Submission Procedures to Ensure that CEII Status is Properly Invoked

The IRC also requests that the Commission and NERC clarify that NERC will continue to comply with the CEII submission requirements in 18 CFR 388.113(d)(1)(i), including the requirement to provide a justification for CEII status, under the proposed submission process. Although the White Paper clearly reflects an intention that the information submitted in the CIP NOP filing attachment will be regarded as CEII, the Commission's rules condition CEII status on the submitter's compliance with various submission requirements, including requirements to properly label the information, request a duration of CEII treatment, and provide a justification for CEII treatment. Failure to properly invoke CEII status under these requirements could jeopardize the protected status of the information. The IRC has no reason to believe that NERC will not continue to comply with these submission requirements, but out of an abundance of caution, requests clarification of that intention.

With respect to the required justification for CEII status, because FERC apparently intends to treat the entirety of the CIP NOP filing attachment as CEII, the IRC suggests that joint staffs either (1) adopt a standard practice in the White Paper under which NERC

would simply recite elements of the definition of CEII in 18 CFR 388.113(c)(2) in each CIP NOP submission as a justification for CEII treatment of the attachment information, or (2) include in the White Paper a statement reflecting the Commission's understanding that the information in the proposed attachment comes within the definition of CEII in 18 CFR 388.113(c)(2), and then establish in the White Paper that NERC would simply reference this statement as the required CEII justification in each future CIP NOP submission.

7. NERC Should Revise its Rules of Procedure to Conform with the White Paper

The IRC submits that changes to the NERC Rules of Procedure will also be needed to conform with the proposal in the White Paper. For example, under the NERC Rules of Procedure, Appendix 4C, section 5.6, when a violation is resolved via settlement, NERC must post on its website "…a copy of the settlement or a description of the terms, and a copy of any Mitigation Plan that is agreed to as part of the settlement…" with any CEII redacted. Under the joint staffs' proposal, any settlement, description of the terms, and mitigation plans will be CEII and, therefore, should not be publicly posted. Other revisions to the NERC Rules of Procedure may also be appropriate and should be addressed through a separate NERC proceeding.

8. NERC Should Develop Alternate Methods to Share Valuable Information

The current Notice of Penalty format provides valuable information to other Registered Entities about potential violations, mitigation options, and the penalty amounts for violations of Reliability Standards involving the same or similar facts and

circumstances, which must be comparable under the NERC Rules of Procedure.[15] If joint staffs adopt the Notice of Penalty format proposed in the White Paper, then Registered Entities would lose some ability to learn from each other about cyber vulnerabilities and mitigation measures because the details that currently are released in the public versions of the Notices of Penalty would instead be treated as CEII and protected from public disclosure. While NERC states in the White Paper that it will ensure that lessons learned from violations are still shared among registered entities, the IRC suggests that NERC, the Commission, and stakeholders explicitly identify alternative means for sharing the information that will become unavailable as a result of any revisions to the format for filing Notice of Penalty. For example, the IRC requests that NERC consider adding a process by which Notices of Penalty are anonymized and maintained in a secure database that can be accessed by Registered Entities through a password-protected page on NERC's website.

To the extent information about violations continues to be publicly disclosed, the IRC is concerned that this information could be used with the identification of the Reliability Standard in the proposed Notice of Penalty filing to identify which entity violated the Reliability Standard, which could undermine the White Paper's goal of protecting this information from public disclosure. This underscores the importance of removing the identification of the Reliability Standard from the cover letter in the Notice of Penalty filing.

[15] *See, e.g.*, NERC Rules of Procedure, § 407 (requiring NERC to review and ensure penalties, sanctions, and remedial action directives are consistent for violations involving the same or similar facts and circumstances.).

D. Related Issues for the Commission's Consideration

The proposal in the White Paper is highly dependent on the ability of the Commission's CEII rules and regulations to protect the information in the Notices of Penalty. However, it is not clear how the Commission determines whether to release CEII to a given requestor or the standard the owner of the information must meet to prevent the Commission from releasing such information.[16] Moreover, the IRC has concerns with the Commission's dependence on non-disclosure agreements as the sole means of protecting the release of CEII information obtained through the Commission's FOIA/CEII processes.[17]

For these reasons and to complement the joint staffs' proposed Notice of Penalty format, the IRC requests that the Commission work with all commenters to this proceeding to address the related concerns noted above.

II. CONCLUSION

In response to the White Paper, the IRC respectfully requests that joint staffs consider the comments contained herein.

[16] There are numerous examples of the RTOs and ISOs objecting to requests made to FERC for the RTOs' and ISOs' CEII information where an individual or entity requesting the CEII merely states that it wants to 'complete studies' or simply describes, without specificity, its plans for a generalized analysis of large portions of the bulk-power system, if not the entire Eastern and Western Interconnections.

[17] Notably, malicious actors are not particularly concerned with the information being made public after it is obtained from the Commission. Rather, they seek the information for their own malicious purposes making the Commission's CEII process relevant once the FOIA process is closed to them. *See* the Commission's CEII process at https://www.ferc.gov/legal/ceii-foia/ceii/eceii.asp; *see also* the Commission's FOIA process at https://www.ferc.gov/legal/ceii-foia/foia/foia-new-form/FOIARequest.aspx.

Respectfully submitted,

/s/ *Chad V. Seely*
Chad V. Seely
Vice President and General Counsel
Nathan Bigbee
Assistant General Counsel
Brandon Gleason
Senior Corporate Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
nathan.bigbee@ercot.com

/s/ *James M. Burlew*
Craig Glazer
Vice President-Federal Government Policy
James M. Burlew
Senior Counsel
PJM Interconnection, L.L.C.
2750 Monroe Boulevard
Audubon, Pennsylvania 19403
james.burlew@pjm.com

/s/ *Robert E. Fernandez*
Robert E. Fernandez, General Counsel
Raymond Stalter, Director of Regulatory Affairs
Carl Patka, Assistant General Counsel
Christopher Sharp, Senior Compliance Attorney
New York Independent System Operator, Inc.
10 Krey Boulevard
Rensselaer, New York 12144
csharp@nyiso.com

/s/ *Maria Gulluni*
Maria Gulluni
Vice President and General Counsel
Margoth R. Caley
Senior Regulatory Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@iso-ne.com

/s/ *Roger E. Collanton*
Roger E. Collanton, General Counsel
Anna McKenna
Assistant General Counsel, Regulatory
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ *Paul Suskie*
Paul Suskie
Executive Vice President, Regulatory Policy & General Counsel
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

/s/ *Andre T. Porter*
Andre T. Porter Vice President, General Counsel and Secretary
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
aporter@misoenergy.org

October 28, 2019