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 MIDCONTINENT INDEPENDENT SYSTEM OPERATOR, INC.

The Midcontinent Independent System Operator, Inc. ("MISO") respectfully submits these comments in response to the Federal Energy Regulatory Commission ("FERC")/North American Electric Reliability Corporation ("NERC") Joint Staff White Paper on Notices of Penalty for Violations of NERC CIP Standards ("White Paper") issued in the above-referenced docket, on August 27, 2019.[1] In the White Paper, FERC and NERC staff proposed, for the first time, public disclosure of entity names, standard(s) violated, and penalty amounts, for settlement agreements and for matters handled pursuant to the Find, Fix and Track program and the Compliance Exception program. This proposal marks a significant change in how FERC and NERC propose to handle public disclosure of resolutions of CIP violations at all violation levels.

I. COMMENTS

MISO appreciates this opportunity to provide comments on the FERC/NERC Staff White Paper on CIP Standards and Notices of Penalty. MISO agrees with the White Paper that a balance must be achieved between public disclosures and security. MISO's comments focus on three aspects of the White Paper proposal:

---

[1] *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).

A. Whether the White Paper strikes the appropriate balance between public disclosures and security;

B. Whether the White Paper addresses adequately security concerns;

C. Whether alternatives to the White Paper approach might better address security concerns.

A. Balance between Disclosures and Security

MISO acknowledges that achieving the appropriate balance between grid security and public disclosure (adding detail such as entity name and CIP standard violated to a "public" cover page) lies at the heart of the White Paper. That question of balance has informed and suffused the administration of NERC CIP Standards from their inception. NERC's current penalty submission practices has been to limit disclosure of details that would provide "a road map for bad actors." Bad actors intend harm to the electric grid and are actively engaged in activities that probe and exploit grid vulnerabilities, to facilitate their attacks. To counter that risk, many entities pursue a two pronged electric grid defense: first, preventing attacks and secondly, delaying, disrupting, detecting, and limiting attacks.

MISO respectfully submits that the addition of any information to already publicly available information enhances a bad actor's ability to home in on and exploit vulnerabilities and focus cyberattacks, particularly when that disclosure links entities with specific NERC CIP standards violations and penalties. For that reason, the proposed addition of publicly available information to include entity names, standards violated and penalties paid raises concerns. Public disclosure of an entity name points a bad actor to a specific region of the grid on which to focus; public disclosure of the CIP Standard violated points a bad actor to specific kinds of vulnerabilities. Even after violations have been mitigated, vulnerabilities may persist, despite the best efforts of entities, the regions and NERC. Directing attention in these ways tends to simplify the work of bad actors, and tends to increase the risk of a successful cyberattack.

The White Paper assumes parity between grid security and public disclosure. MISO questions whether such parity should be assumed, in a world where bad actors pore over publicly available information to shortcut their identification of vulnerabilities for cyberattack. Public disclosure of heretofore protected information absent a compelling purpose for disclosure removes a key grid defense strategy – delay. For these reasons, the White Paper's rebalancing of security and disclosure is problematic and merits reconsideration.

B. On-Going Security Concerns

The White Paper generally reflects the assumption that public disclosure is a helpful tool to further protect the electric grid. It is worth noting that the electric industry already stands alone among industries in having mandatory and enforceable cyber security standards. The White Paper suggests a step of disclosure over and above the enforcement of those standards as beneficial to the industry and public. MISO does not believe such disclosure supports needed grid reliability. To further assess the potential risks associated with the disclosures as proposed in the White Paper, MISO respectfully requests that FERC consider outreach to other agencies of the federal government that have even broader cyber defense and cybersecurity responsibilities than FERC's and NERC's. Entities like MISO hear frequently, for example, from representatives from their regional FBI and their Departments for Homeland Security (federal and state) about the need to limit publicly available information, as a means of maintaining and enhancing cybersecurity for the electric grid. Entities like MISO collaborate with these security-focused federal and state agencies, and these voices add an important element to consideration of these White Paper disclosure proposals.

And, MISO respectfully submits that a more fulsome consideration of security concerns is warranted here, given the risks that disclosures of additional information pose to the electric grid. For example, MISO respectfully suggests that the more general question of whether

FERC's current approach to the handling of CEII adequately protects the grid should be part of these deliberations. CEII disclosure processes, which even five or ten years ago may have adequately protected critical electric infrastructure information, do not consider the immediate threats from disclosure. A requestor's non-disclosure agreement and explanation of proposed uses of CEII (without detailed explanations of CEII storage and protection arrangements, for example) provide no real protection for the electric grid, especially if that disclosed CEII should fall into the possession of a bad actor.

This stark reality may leave front line protectors of CEII, utilities and ISO/RTOs, with the uncomfortable and dangerous reality that providing information to FERC may increase the risks of cyberattacks on the electric grid, if disclosure of entity names and NERC CIP Standards violated becomes the norm.

While most entities track attempts to access entity systems, no entity can track attempts or incursions that never occurred because a bad actor's work was slowed by not having access to entity names and NERC CIP standards violated. Unfortunately, if the White Paper approach is adopted without changes, entities indeed may be able to point to attempts or incursions hastened by the newly publicly available information on entity name and standards violated, but that would be, at best, a Pyrrhic victory.

C. Opportunities for Alternatives to Better Address On-Going Security Concerns

MISO considers the White Paper proposal a sound starting point for a real discussion of cybersecurity and public disclosures. MISO offers the following suggestions for the Commission's consideration of alternatives to the White Paper proposal.

First, a more fulsome review of CEII, including in that context both a consideration of NERC CIP settlement agreement disclosures AND consultations with other federal agencies tasked with cyber defense and cybersecurity.

Secondly, if the full review of CEII is not feasible, and the focus remains disclosure of entity names, NERC CIP Standards violated, and Notices of Penalty, MISO proposes consideration of an annual or semi-annual list of entities that have settled violations and the aggregate penalty collected from that group of entities, with no reference to the specific NERC CIP Standard violated. This approach would disclose additional information to the public without providing an enhanced road map for bad actors. And, MISO would suggest that such a listing omit compliance exceptions and find, fix, track matters because those matters pose low risk to the electric grid, by definition. Entities look to the currently available anonymous descriptions of compliance exceptions and find, fix, track matters as a means of checking their own compliance vulnerabilities; this practice enhances overall grid security, and enhances cybersecurity alignments among entities. This practice also discloses information to the public on how entities are finding and addressing cyber vulnerabilities.

Third, in lieu of disclosures around Compliance Exceptions and Find, Fix, Track matters, MISO proposes an annual list of standards arranged from “most violated” to “least violated” of the kind already compiled by the regions, which would provide insights to entities and the public without providing an enhanced road map to violators.

II. COMMUNICATIONS

Communications and correspondence regarding this filing should be directed to:

Mary-James Young
Midcontinent Independent
System Operator, Inc.
720 City Center Drive
Carmel, IN 46082-4202
Telephone: 317.249.5400
myoung@misoenergy.org

MISO has served all parties provided in the Commission's eService list for the above referenced docket. In addition, MISO notes that it has served a copy of this filing electronically, including attachments, upon all Tariff Customers under the Tariff, MISO Members, Member representatives of Transmission Owners and Non-Transmission Owners, as well as all state commissions within the Region. In addition, the filing has been posted electronically on MISO's website at https://www.misoenergy.org/legal/ferc-filings/ for other parties interested in this matter.

III. CONCLUSION

MISO appreciates this opportunity to comment on the White Paper proposal. MISO respectfully submits that additional consultations and considerations would materially improve both cyber defense and cybersecurity. Those should include consideration of an expanded review of CEII generally (and not just in the context of NERC CIP settlement agreements), as well as consultations with other federal agencies responsible for cyber defense and cybersecurity. To that end, MISO urges the Commission to consult with federal agencies like the FBI and the Department of Homeland Security, both of which work regularly with registered entities on matters related to cybersecurity, and both of which can provide insights into cyber defense and cybersecurity, and speak to the risks to entities and the electric grid inherent in providing more publicly available information on NERC CIP violations.

Additionally, MISO urges the Commission to reconsider the aspect of the White Paper that proposes to disclose entity names, NERC CIP Standard(s) violated and penalty amounts. An annual or semiannual list of settling entities with an aggregated penalty amount and no mention of the specific standard violated is an alternative that merits further consideration.

Respectfully submitted,

/s/ Mary-James Young
Mary-James Young
Midcontinent Independent
System Operator, Inc.
720 City Center Drive
Carmel, IN 46082-4202
Telephone: 317.249.5400
myoung@misoenergy.org

Attorney for the
Midcontinent Independent
System Operator, Inc.

Dated: October 28, 2019

CERTIFICATE OF SERVICE

I hereby certify that I have this day e-served a copy of this document upon all parties listed on the official service list compiled by the Secretary in the above-captioned proceeding, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2012).

Dated at Carmel, Indiana this 28th day of October, 2019.

/s/ Julie Bunn
Julie Bunn
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
Telephone: (317) 249-5400

Document Content(s)