

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Joint Staff White Paper on)
Notices of Penalty Pertaining to) Docket No. AD19-18-000
Violations of Critical Infrastructure)
Protection Reliability Standards)

COMMENTS OF THE
NEW HAMPSHIRE OFFICE OF THE CONSUMER ADVOCATE

The New Hampshire Office of the Consumer Advocate (NH OCA) hereby submits the following comments in response to the August 27, 2019 Notice seeking responses to the document entitled “Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards” (Staff White Paper) as issued by the FERC Staff in conjunction with the Staff of the North American Electric Reliability Corporation (NERC). For the reasons that follow, the NH OCA respectfully urges the FERC to embrace the premise of the Staff White Paper – that applicable law and public policy require more transparency when it comes to violations of critical infrastructure reliability standards – while going beyond the relatively modest reforms the White Paper actually proposes.

I. About the New Hampshire Office of the Consumer Advocate

Pursuant to N.H. RSA 363:28, II, the NH OCA is tasked with representing the interests of the Granite State’s residential utility customers “in any proceeding

concerning rates, charges, tariffs, and consumer services before any board, commission, agency, court, or regulatory body in which the interests of residential utility customers are involved.” Although retail rate cases and other matters within the jurisdiction of the New Hampshire Public Utilities Commission are the bread and butter of the NH OCA’s work, we regularly participate in FERC proceedings. In addition, the NH OCA is an end-user member of NEPOOL, the official stakeholder advisory forum of the regional transmission organization ISO New England, which operates the bulk power transmission system and wholesale electricity markets of the six New England states.

Our involvement in regional and national matters is premised on the notion that many if not most key decisions, concerning not just rates but also the safety, reliability, flexibility and technological capabilities of electric service provided to consumers in New Hampshire, are made at the regional and federal levels. Additionally, we are an active participant in the investigative docket the New Hampshire Public Utilities Commission opened in 2015 on the subject of grid modernization (N.H. PUC Docket No. IR 15-296). Progress in that docket has been slow to achieve, and it has become apparent that concerns about cybersecurity are the principal reason New Hampshire has yet to adopt a new roadmap for grid modernization and electric distribution planning generally. We thus believe that it is important for our office to participate actively when matters related to cybersecurity and the protection of critical infrastructure come before regulators and other decisionmakers.

II. Appropriately calibrated transparency is a key element of cybersecurity.

As noted in the Staff White Paper, the issue under examination in this docket is a straightforward one: How transparent should the FERC be when it receives a Notice of Penalty (NOP) from NERC in its capacity as the FERC-certified electric reliability organization pursuant to section 215(c) of the Federal Power Act, 16 U.S.C. § 824o(c)? The Federal Power Act authorizes NERC to impose a penalty on a user, owner, or operator of the FERC-jurisdictional bulk power system, subject to review by the FERC upon receipt of the NOP and a timely request from the alleged violator. *See* Staff White Paper at 5. Specifically at issue here are alleged violation of reliability standards related to critical infrastructure protection (CIP) – i.e., cybersecurity. *Id.* at 2.

According to the Staff White Paper, the FERC’s rules require the agency to treat as confidential anything contained in such NOPs based on the mere assertion by NERC that the information is CEII – i.e., critical energy/electric infrastructure information – “until such time as Commission staff finds that the information is not entitled to such treatment.” *Id.* (citations omitted). Before 2018, this had the effect of shielding from public scrutiny essentially everything about cybersecurity violations described in NOPs, even the identity of the violators. *Id.* at 3. Then came the first of what proved to be a blizzard of requests for disclosure pursuant to the Freedom of Information Act. *Id.* This, in turn, led to the disclosure of the identity of violators “in some limited cases where the Commission staff has determined that

the release will not jeopardize the security of the Bulk-Power System if publicly disclosed.” *Id.*

As one of her final acts a member of the FERC, Commissioner Cheryl LaFleur expressed concern about the “growing controversy” over the transparency of CIP-related NOPs and observed that “state regulators, members of the public, and others have a legitimate interest in such violations” such that the agency “should seek to achieve as much transparency as [it] can consistent with protecting legitimate security interests.” Statement of Commissioner LaFleur (Aug. 27, 2019). Nevertheless, the Staff White Paper does not propose any revisions to the applicable FERC rules. It merely suggests an informal update of the format NERC uses to submit NOPs, so that such notices “would consist of a proposed public cover letter that discloses the name of the violator, the Reliability Standard(s) violated . . . and the penalty amount.” Staff White Paper at 3; *see also id.* at 10 (clarifying that the disclosure of which Reliability Standard or Standards had been violated would not include disclosure of “the requirement or sub-requirement violated”).

The reforms proposed in the Staff White Paper are necessary but not sufficient if the Commission is to achieve the goal described by former Commissioner LaFleur of achieving an appropriate balance between legitimate cybersecurity interests and the principles of openness and public accountability enshrined in the Freedom of Information Act. The need for transparency is all the more acute in these particular circumstances; via Section 215(c) of the Federal Power Act and the FERC’s designation of an industry-sponsored organization

(NERC) as the nation's primary reliability watchdog, the federal government has substantially privatized an essential public function subject to carefully circumscribed oversight from the FERC. Thus, the remainder of these comments explain why the Commission should go beyond the recommendations contained in the Staff White Paper.

III. The Commission should adopt the Mabee alternative proposal.

The NH OCA urges the Commission to adopt the approach outlined in the September 3, 2019 pleading entitled "Comments and Alternate Proposal" and submitted by Michael Mabee of Mont Vernon, New Hampshire. As Mr. Mabee noted, the proposal contained in the Staff White Paper does not provide for the public disclosure of enough information "to allow for public, investor, Congressional and state scrutiny and evaluation of the violators and the regulatory system." Mabee Comments and Alternate Proposal at 5; *see also* September 26, 2019 letter from Reporters Committee for Freedom of the Press at 2 ("Meaningful oversight, accountability, and reform are predicated on the ability of the press and public to examine and scrutinize government records"). Mr. Mabee proposes that the FERC go beyond the mere disclosure of names, standards violated, and the penalties imposed and instead make publicly available these seven specific items:

- All information fields contained in the present Searchable NOP Spreadsheet used by NERC, including the name of the entity that committed the violation,
- The date on which the violation was discovered,
- The duration of the violation,

- The manner in which the violation was discovered,
- A description of the violation in plain English,
- Aggravating and mitigating factors bearing on the penalty assessment, and
- Any settlement agreement applicable to the NOP.

Mabee Comments and Alternate Proposal at 5. Mr. Mabee lays out in persuasive fashion the specific reasons why the disclosure of this specific constellation of information aids the cause of accountability. *See id.* at 5-11 (referring, *inter alia*, to regional violation patterns, the meaningful use of relational databases, evaluation of the effectiveness of the enforcement regime, statistical analysis, etc.). He notes that merely disclosing the reliability standard that was violated, without revealing the requirement or sub-requirement violated, is to provide information at such a level of bland generality as to be meaningless for purposes of public scrutiny. *Id.* at 7-9. He notes that these disclosures provide would-be cyber-no-goodniks no actionable information – and that, should there be any legitimate concerns to the contrary in any specific case, NERC can and should make a showing to that effect which would allow the FERC to redact information on a case-by-case basis. This is a very sound approach because it places the presumption where it belongs – in *favor* of disclosure.

Our experience, as a frequent litigant before the New Hampshire Public Utilities Commission and as an end-user member of NEPOOL (the stakeholder advisory board to the regional transmission organization ISO New England) is that electric utilities (i.e., the same firms that own the bulk power transmission system)

consistently rely on conclusory and self-serving allegations about the ill-effects of transparency to thwart efforts to hold them and their regulators publicly accountable. We see it at the state level when utilities claim, without proof, that they would suffer competitive harm by certain disclosures even though they are regulated monopolies. We see it at the regional level when industry insiders claim that opening their deliberations as RTO stakeholders would have a chilling effect on their discussions. *See, e.g., RTO Insider LLC v. New England Power Pool Participants Committee*, 167 FERC ¶ 61021 (2019) (concurring statement of Commissioner Glick) (“To paraphrase Justice Louis Brandeis, sunlight is the best disinfectant and it is hard for me to understand how barring public and press scrutiny will further NEPOOL’s mission or, ultimately, its legitimacy as the forum for considering how ISO New England’s actions affect its stakeholders”).¹ And we see it here.

We do not begrudge utilities the opportunity to make these assertions, nor do we necessarily contend that all or even most such claims of harm or potential harm are meritless. Our point is merely to caution the FERC not to rely on such positions when unsupported by evidence or even arguments that go beyond tautologies. From the ratepayer perspective, such caution is especially warranted when the subject is cybersecurity. Cyber-threats have emerged as the excuse of the century for billions

¹ Commissioner Glick also observed: “Rather than trying to hide their discussions from the public, NEPOOL and its members would be better served by permitting public and press attendance, so that all entities—including those that cannot spend the time or money needed to attend all NEPOOL meetings—can remain informed of the discussions regarding the important issues under NEPOOL’s purview. That result would lead to a more robust discussion of the issues and, ultimately, to better public policy.”

and billions of dollars in new utility investments in circumstances that conveniently evade the traditional public scrutiny for prudence, used-and-usefulness, etc. In New Hampshire, the pending “grid modernization” investigation at the NH PUC is rife with claims by utilities that they should be allowed to make massive investments in cybersecurity defenses subject to automatic cost recovery whose scrutiny will occur, if at all, behind closed doors. *See* New Hampshire Public Utilities Commission, *Staff Recommendation on Grid Modernization* (Jan. 31, 2019) at 75 (calling for utility submission of integrated distribution plans for regulatory approval that do “not contain specific measures that may compromise the utility’s security plan” but describe only a “high level approach in addressing cyber security and privacy in the various layers of the utility’s system”).² But we are reliably told by the utilities with which we have frequent contact that their systems are queried by potential cybercriminals repeatedly throughout every day. In these circumstances, it is simply not tenable for the FERC to conclude that the modest disclosures suggested by Mr. Mabee would give sophisticated cyber-criminals actionable information they do not already have.

IV. Conclusion

The Staff White Paper referenced four issues deemed relevant to the decision at hand: (1) potential security benefits, (2) potential security concerns, (3) implementation difficulties, and (4) “whether the proposed format provide[s]

² The referenced document was filed in New Hampshire PUC Docket No. IR 15-296 and is available at https://www.puc.nh.gov/Regulatory/Docketbk/2015/15-296/LETTERS-MEMOS-TARIFFS/15-296_2019-02-12_STAFF_REPORT_AND_RECOMMENDATION.PDF.

sufficient transparency to the public.” Staff White Paper at 4. For the reasons described above, the proposal contained in the Staff White Paper is laudable but ultimately inadequate to the needs of transparency and accountability. We respectfully request that the FERC put commenters with different perspectives to their proof by requiring them to come forward with persuasive evidence of security concerns implicated by the proposals in the Staff White Paper and Mr. Mabee’s comments. Please do not let entrenched industry insiders use cybersecurity scare tactics to justify shielding them from public accountability.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read 'D. Maurice Kreis', written in a cursive style.

D. Maurice Kreis
Consumer Advocate

Office of the Consumer Advocate
21 South Fruit Street, Suite 18
Concord, New Hampshire 03301
603.271.1174 (direct line)
donald.kreis@oca.nh.gov

October 25, 2019

Document Content(s)

oca comments 191025.PDF.....1-9