Before the
UNITED STATES OF AMERICA
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 DAVID JONAS BARDIN ON RELATION OF THIS DOCKET TO TWO CULTURES: "COMPLIANCE" AND "BEST PRACTICES"

(September 18, 2019)

1. I respond, as a citizen, to the Commission's August 27, 2019, Notice of White Paper [1] mindful that

- Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC) staffs issued a joint White Paper to address NERC's submission, and FERC's processing, of Notices of Penalty (NOPs) for Critical Infrastructure Protection (CIP) Reliability Standards violations;
- "[t]he opinions and views expressed in this staff White Paper do not necessarily represent those of the [FERC], its Chairman, or individual Commissioners, and are not binding on the Commission. Similarly, the opinions and views expressed [fherein] do not necessarily represent those of the NERC Board of Trustees, its chair, or any individual trustee, and are not binding on them."

Staffs' joint White Paper narrowly describes the context of NERC and FERC procedures at issue in this docket (focusing on issues stemming from over-designations under FERC's Critical Energy/Electric Infrastructure Information (CEII) regulations which "staff did not assess" until 2018). [2]

---

[1] See https://elibrary.ferc.gov/idmws/common/downloadOpen.asp?downloadfile=20190827%2D4000%2833759968%29%2Epdf&folder=16764990&fileid=15335254&trial=1.

[2] See PG*&E Identified as Utility That Lost Control of Confidential Information. As a result of 2016 failure, 30,000 records about PG&E's cyber assets were exposed on the internet* (Wall Street Journal, August 24, 2018) at https://www.wsj.com/articles/pg-e-identified-as-utility-that-lost-control-of-confidential-information-1535145850. Staffs' joint White Paper states:

(a) that CIP NOPs, as submitted to FERC by NERC, "typically include information pertaining to the nature of the violation, potential vulnerabilities to cyber systems as a result of the noncompliance, and mitigation activities. Information useful to a person in planning an attack on critical electric infrastructure may be subject to the Commission's Critical Energy/Electric Infrastructure Information (CEII) regulations and/or 18 CFR § 39.7(b)(4)" [providing "The disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that the security of the Bulk-Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise"];

(b) that "NERC's practice has been to request certain information in CIP NOPs, including the identity of the violator be designated as non-public and CEII pursuant to [FERC's] rules and regulations";

(c) that FERC's "practice, as set forth in its rules and regulations, is to treat information asserted to constitute CEII as non-public, without designating it as such, until such time as [FERC] staff finds that the information is not entitled to such treatment";

(d) that FERC "staff does not make determinations on NERC's requests for CEII designation at the time of filing; however, the information is maintained as non-public in [FERC's] filing system, eLibrary, until such time as [FERC] staff determines that it is not entitled to CEII treatment (e.g., in response to a third-party information requests)"; and

(e) that FERC "staff did not assess a NERC request for CEII designation until 2018 when, for the first time, [FERC] received a FOIA request seeking the name of an undisclosed CIP violator (referred to by NERC as an "unidentified registered entity" or "URE")."

2. I am also mindful of observations by Commissioner LaFleur on August 27, 2019, [3] and Commissioner Glick (in Docket No. NP19-4) on August 29, 2019. [4]

3. Commissioner Glick stated (footnotes omitted):

> "[FERC's] Notice denies the motions to intervene from multiple parties who have requested that [FERC] name the unidentified registered entity (URE) that is the subject of the Notice of Penalty (NOP). Although I agree with the decision to deny the motions to intervene, the parties seeking intervention raised important issues concerning the lack of transparency associated with the [NERC] NOP process.
>
> "It is essential that we sufficiently incent entities to comply with the [CIP] standards. Certainly these entities would be encouraged to comply in order to avoid substantial fines. But it is also important that those entities that violate CIP standards, especially entities responsible for numerous and significant violations, be publicly identified in order to provide an additional deterrent. Such transparency would encourage management to take appropriate actions to avoid the attention that comes with being publicly identified as having significantly violated CIP standards.
>
> "The current NOP process makes it difficult for [FERC] to provide for a necessary level of transparency because [FERC] must also ensure that we are not inadvertently providing information useful to someone seeking to attack critical electric infrastructure. Under the current approach, it is possible that identifying an offending party ... might also reveal weaknesses in the entity's process for protecting critical infrastructure, inadvertently exposing the bulk power system. I am pleased that [FERC] and NERC staff earlier this week released a White Paper proposing a path forward to better balance the need for confidentiality to protect system security with the benefits associated with transparency. This White Paper proposes that generally NOPs will identify the offending party but omit sensitive information that could expose their systems to exploitation. I encourage interested parties, including those that sought to intervene in this NOP proceeding, to participate in the White Paper docket as [FERC] works to address ongoing concerns regarding transparency and security of the NERC NOP process."

4. Commissioner LaFleur stated that "handling and confidentiality of these NOPs has been an issue of growing controversy. ... [I]t is essential that FERC and NERC conduct public process to consider the appropriate balance between transparency and security in these instances. ..."

> "The procedures that NERC and FERC have followed in processing NOPs for CIP violations has been in place since before I joined FERC and has not been changed in the past decade, ... I think it is highly appropriate that we consider changes to the process at this time. [I]t is important that we handle NOPs so as to avoid subjecting the bulk electric system to risk of a cyber attack once a vulnerability is identified. TAt the same time, I believe state regulators, members of the public, and others have a legitimate interest in such violations, and we should seek to achieve as much transparency as we can consistent with protecting legitimate security interests.
>
> "I believe the FERC and NERC staff have put forth one proposal worthy of consideration for a way to handle these NOPs differently. I hope that we receive a wide range of comments on the

---

[3] See https://elibrary.ferc.gov/idmws/common/downloadOpen.asp?downloadfile=20190827%2D4001%2833760378%29%2Epdf&folder=16765903&fileid=15335449&trial=1.

[4] See https://elibrary.ferc.gov/idmws/common/downloadOpen.asp?downloadfile=20190829%2D3055%2833765290%29%2Epdf&folder=16843761&fileid=15337526&trial=1.

> White Paper, including any suggestions for alternative processes, which will allow FERC and NERC to move forward on this issue."

5. Michael Mabee submitted an alternative proposal on September 3, 2019. [5] George R. Cotter submitted complementary comments dated September 6, filed September 12, 2019. [6] Others may follow. The Commission (and NERC) should weigh alternatives in multiple contexts, as outlined below.

6. Background. The Commission would do well (especially in light of turnovers) to lay out more fully than does the joint White Paper how these NOP procedures came to be:

- Why did FERC and NERC impose mandatory CIP standards, enforceable by penalties for violations, in the first place (instead of relying solely on voluntary good and "best" practices)?
- In addition to enforcing compliance with these minimal, mandatory FERC/NERC CIP standards, what do FERC, NERC, and others — including Instititute of Nuclear Power Operations (INPO) and Federal Bureau of Investigation (FBI) — do to encourage and foster voluntary "best practices"?
- Are FERC/NERC minimal, mandatory CIP standards as limited as Mr. Cotter concludes? [7] To extent they are, why were they made so limited?
- Under current FERC/NERC practices, do Departments of Energy (DoE), Homeland Security (DHS), Justice (DoJ) and other federal authorities — e.g., Nuclear Regulatory Commission (NRC), Securities and Exchange Commission (SEC), The National Counterintelligence and Security Center (NCSC)— receive data at issue here even if withheld from investors, state regulators, journalists, general public?
- What detailed analyses have FERC or NERC published using anonymous NOP data at issue here?
- Could FERC/NERC procedures at issue here apply to cyberattack incident(s) reported by E&E News on September 6, 2019, [8] and to same and earlier incidents discussed by Joe Weiss on September 8, 2019? [9]

7. Spectrum of contexts. Narrowest context would disregard everything except limited way in which FERC and NERC exercised mandatory powers to set CIP Standards. (That might seem a "lawyer-like" context.) Broader contexts would consider (a) entire range of potential FERC and NERC mandatory standard setting powers under Federal Power Act, or (b) all electric industry cybersecurity issues, whether covered by Federal Power Act or not (e.g. distribution) and voluntary "best practices" advocacy as well as mandatory standards. [10] (c) Broadest of all would consider context of significant cyber vulnerabilities of all important industries and a rapidly changing world.

---

[5] See https://elibrary.ferc.gov/idmws/common/downloadOpen.asp?downloadfile=20190903%2D5033%2833768996%29%2Epdf&folder=16766509&fileid=15340441&trial=1.

[6] See https://elibrary.ferc.gov/idmws/common/downloadOpen.asp?downloadfile=20190912%2D0014%2833795044%29%2Epdf&folder=16845269&fileid=15355490&trial=1.

[7] See pp. 7-8 of Mr. Cotter's Attachment, concluding: "CIP Standards have had no value in protecting the Grid from foreign adversaries; ... . The major reasons the Grid has been an easy Russian target are (1) how few cyber assets are covered under CIP Standards, (2) the exclusion of communications and network linkages despite extensive Internet connectivity by utilities, (3) the absence of hard technical requirements in standards, and (4) the extremely weak compliance system in use." See also Appendix II to his Attachment.

[8] "A first-of-its-kind cyberattack on the U.S. grid created blind spots at a grid control center and several small power generation sites in the western United States, according to a document posted yesterday from the [NERC]. See https://www.eenews.net/stories/1061111289.

[9] *The US electric grid has been cyber attacked for years yet NERC won't acknowledge facts* at https://www.controlglobal.com/blogs/unfettered/the-us-electric-grid-has-been-cyber-attacked-for-years-yet-nerc-wont-acknowledge-facts/.

[10] See, for example, FBI, *Best Practices for Victim Response and Reporting of Cyber Incidents* (DOJ FBI Cybersecurity Unit, February 2018) at https://www.justice.gov/criminal-ccips/file/1096971/download. The FBI may be able to share more recent guidance with FERC and NERC staffs.

8. Context of SEC guidance, The SEC's *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (2018) [11] — which probably applies to many entities that are subject to procedures at issue here and their NOPs — includes:

> "Cybersecurity risks pose grave threats to investors, our capital markets, and our country.
>
> ....
>
> "This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts – for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident. Nevertheless, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale of securities and to take steps to prevent directors and officers (and other corporate insiders who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk." [Pages 1, 11-12, footnotes omitted]

9. Context of ongoing, decades-long cyber struggles. The Commission would do well to consider an even broader context (and national security community perspectives on it), as explained by Glenn S. Gerstell, general counsel of the National Security Agency (NSA) on September 10, 2019, in the NY Times [12] — even though NSA is unlikely to deal with domestic cyberattack issues.

10. I respectfully ask the Commission to take official notice of Mr. Gerstell's article. His observations include the following:

- "[Our national security] early-warning centers have *no ability to issue a warning* to the president that would stop a *cyberattack that takes down a regional or national power grid* ..." [emphasis added]
- "[T]he intelligence community and its allies who rely on one another for information-sharing must now adapt to adversaries with new capabilities — *principally China, Russia, Iran and North Korea*, each of which presents different and complex threats — ... ." [emphasis added]
- "There are four key implications ... :"
  > "The first is that the unprecedented scale and pace of technological change will outstrip our ability to effectively adapt to it."
  >
  > "Second, we will be in a world of *ceaseless and pervasive cyberinsecurity and cyberconflict* against nation-states, businesses and individuals." [emphasis added]
  >
  > "Third, the flood of data about human and machine activity will put such extraordinary economic and political power in the hands of the private sector that it will transform the fundamental relationship, at least in the Western world, between government and the private sector."
  >
  > "Finally, and ... ominously, the digital revolution has the *potential for a pernicious effect on the very legitimacy and thus stability of our governmental and societal structures*." [emphasis added]

---

[11] See https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[12] *I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution. (Technology is about to upend our entire national security infrastructure.)* at https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html?login=email&auth=login-email.

- "It is by no means assured that our national security sector will be able to attract on a sufficient scale the scarce engineering, mathematical and scientific talent that would supply the necessary expertise."

- "We must prepare for a world of *incessant, relentless and omnipresent cyberconflict* — in not only our national security and defense systems (where we are already used to that conflict) but also, more significantly, *every aspect of our daily and commercial lives*." [emphasis added]

- "The sensors, systems, networks, algorithms and machines that will empower our new lives ... will all be part of the Internet of Things. One consequence is that the current division between cyberdefense (think firewalls, penetration testing and cyberhygiene) and supply-chain risk management (think of the assessment of equipment manufacturing, component assurance and availability and surveillance concerns in equipment) will be eliminated, with everyone concerned with the *holistic sanctity of equipment and software to achieve the well-recognized triad of availability, security and integrity*." [emphasis added]

- "[O]ur citizens and businesses will have to accept that *cybermalevolence is a persistent threat, not a war to be won or a disease to be cured.*" [emphasis added]

- "Until recently, at least in the United States, our notions of privacy have been rooted in the Fourth Amendment's delineation of the federal government's powers vis-à-vis the individual citizen. But *what do our notions of privacy mean anymore ...?*" [emphasis added]

11. Conclusions. (a) We can empathize with instinctive desires for privacy that may lead some to oppose transparency recommended by the joint White Paper, but it is hard to imagine how this Commission might fail to make disclosure of violator identities a general (rather than exceptional) case. [13]

(b) The Commission should also assure (i) that categories of detail now being made public (and reflected in the columns of Mr. Mabee's Exhibit A) continue to be publicly available (unless objectors demonstrate a specific problem as to any one of them) and (ii) that these data are used to understand trends.

(c) The Commission should ask entities which already make meaningful and practical disclosures — following SEC guidance and the joint White Paper's recommended transparency culture — to encourage other entities with a different culture to follow suit.

(d) The Commission should review the balance between between minimally acceptable compliance culture and best efforts culture and their respective demands for scarce technical human resources. In addition to administering aspects of mandatory CIP Standards at issue here, the Commission should encourage robust best practices going beyond minimal standards — with enough public information to demonstrate what is really happening to protect bulk power supply and the entire electricity industry.

(e) Why did it take so long for FERC to review and reject NERC's over-designation summarized at footnote 2? Is it a matter of staffing, organization, and/or policy at FERC? at NERC? Do FERC's CEII regulations themselves unduly burden regulated entities, inhibit evolution of best practices, and create excessive demands for scarce resources? Can CEII experience of DoE and other agencies suggest useful improvements?

Respectfully submitted, *David Jonas Bardin* [davidbardin@aol.com]

---

[13] Shakespeare lovers might analogize empathy evoked for Sir John Falstaff's instincts simultaneously with respect evoked for Prince Hal's sense of duty to the contrary.

Document Content(s)