Document Accession #: 20200923-4001 Filed Date: 09/23/2020

SECOND JOINT STAFF WHITE PAPER ON NOTICES OF PENALTY PERTAINING TO VIOLATIONS OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

DOCKET NO. AD19-18-000
September 23, 2020

FEDERAL ENERGY REGULATORY COMMISSION
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The opinions and views expressed in this staff White Paper do not necessarily represent those of the Federal Energy Regulatory Commission, its Chairman, or individual Commissioners, and are not binding on the Commission. Similarly, the opinions and views expressed herein do not necessarily represent those of the NERC Board of Trustees, its chair, or any individual trustee, and are not binding on them.

I. Introduction

On August 27, 2019, the staffs of the Federal Energy Regulatory Commission (Commission) and the North American Electric Reliability Corporation (NERC) issued a joint White Paper (First Joint White Paper) containing a proposal regarding NERC's submission, and the Commission's processing, of Notices of Penalty (NOPs) for violations of Critical Infrastructure Protection (CIP) Reliability Standards. The First Joint White Paper proposed that, going forward, CIP NOP submissions would consist of a public cover letter that discloses the name of the violator, the CIP Reliability Standard(s) violated (but not the Requirement(s)), and the penalty amount.[1] Under the proposal, NERC would submit the remainder of the CIP NOP filing, with details of the violation(s), mitigation activity, and potential vulnerabilities to cyber systems, as a non-public attachment along with a request that such information be designated Critical Energy/Electric Infrastructure Information (CEII). The First Joint White Paper invited comments on the proposal. In response, 77 sets of comments were filed by utilities, industry groups, private citizens, and state and federal government entities.

This Second Joint White Paper was prepared by the staffs of the Commission and NERC following a review of the comments. In view of the tangible risks of publishing CIP violator names and other information found in CIP noncompliance submissions, the First Joint White Paper proposal is insufficient to protect the security of the Bulk-Power System and does not implement the Commission's full legal authority to shield such information from public disclosure. Accordingly, going forward, CIP noncompliance filings and submittals by NERC will request that the entire filing or submittal be treated as CEII and Commission staff will designate such filings and submittals as CEII in their entirety. Additionally, because of the risk associated with the disclosure of CIP noncompliance information, NERC will no longer publicly post redacted versions of the CIP noncompliance filings and submittals.

II. First Joint White Paper

In response to an unprecedented number of requests under the Freedom of Information Act (FOIA), the First Joint White Paper sought to strike a balance between the security and transparency concerns within industry and the general public regarding the disclosure of CIP noncompliance information.[2] The First Joint White Paper proposed to accomplish this by limiting the disclosure of CIP noncompliance information to the name of the violator, the Reliability Standard(s) violated (but not the Requirement), and

[1] The First Joint White Paper indicated that the proposal would also apply to future CIP noncompliance submissions (i.e., Spreadsheet NOPs (SNOPs), Find, Fix and Track submissions (FFTs) and Compliance Exceptions (CEs)). First Joint White Paper at 3 n.5.

[2] 5 U.S.C. § 552 (2018).

the penalty amount. The First Joint White Paper proposed the revised format to seek to balance security and transparency concerns by creating a format for releasing information that, considered on its own, was unlikely to pose a security risk, while withholding information that was more likely to pose a security risk. The revised format also was proposed to create efficiencies in the submission and processing of CIP noncompliance and lessen the potential for inadvertent disclosure of non-public information.

The First Joint White Paper acknowledged that the public identification of CIP violators may result in increased hacker activity, such as scanning of cyber systems and possible phishing attempts. However, the First Joint White Paper expressed the belief that the limited information provided in the proposed cover letter would not provide an adversary with enough information to stage a focused attack on a violator's cyber assets.

The First Joint White Paper sought public comment on the proposal regarding: (1) the potential security benefits from the proposed format; (2) any potential security concerns that could arise from the new format; (3) any implementation difficulties or concerns that should be considered; and (4) if the proposed format provided sufficient transparency to the public.

III. Summary of Comments on the First Joint White Paper

Few commenters supported the First Joint White Paper proposal without seeking modifications to either expand or reduce the amount of information that would be publicly disclosed.[3] Comments submitted by private citizens, state representatives, and consumer advocate offices supported more disclosure of CIP noncompliance information. By contrast, most industry commenters and trade organizations raised concerns with at least some of the proposed disclosures because of the increased risk to the security of the Bulk-Power System.

Commenters supporting additional disclosure of CIP noncompliance information contend that public disclosure is necessary as "companies and regulators will have the proper incentive to work harder on CIP standard compliance."[4] In addition, commenters

[3] DeNexus, Inc., Public Citizen, Reporters Committee for Freedom of the Press, New York Power Authority, Connecticut Public Utilities Regulatory Authority/Connecticut Office of Consumer Counsel, Louisiana Public Service Commission, New Jersey Board of Public Utilities, and Jonathan Appelbaum support the First Joint White Paper proposal without modification.

[4] *See*, *e.g.*, Mabee Initial Comments at 5.

supporting more disclosure assert that it provides the public with the means to understand why violations occur[5] and that the public has a "right to know."[6]

Comments from registered entities and trade organizations raised concerns with some of the disclosures proposed in the First Joint White Paper.[7] The concerns were primarily two-fold. First, identifying the registered entity's name and the Reliability Standard violated could increase the number and success of focused cyber-attacks.[8] And second, unlike the current CIP NOP format, which discloses information that is helpful to other utilities for improving their compliance programs and security efforts, the proposal articulated in the First Joint White paper would keep such information non-public.[9] The comments warn that disclosing a registered entity name in connection with CIP noncompliance would "increase the likelihood that malicious actors could identify and target a Registered Entity's problem areas"[10] without sufficient justification for the increased risk other than the "general benefit of increasing transparency."[11] These commenters state that making a clear connection between the registered entity and the standards at issue paves a "readily accessible path for bad actors."[12] Further, commenters point out that it is unclear how releasing the proposed raw data would improve the

[5] *See, e.g.,* Reitman Comments at 2.

[6] *See, e.g.,* Monahan Comments at 1; Waller Comments at 2-3; Reporters Committee at 2.

[7] Edison Electric Institute, the American Public Power Association, the National Rural Electric Cooperative Association, the Large Public Power Council, the Transmission Access Policy Study Group, the Electric Power Supply Association, and the Electricity Consumers Resource Council (Joint Trade Associations), ISO-RTO Council, MISO, Georgia System Operations Corporation (GSOC) and Georgia Transmission Corporation (GTC), Cogentrix, North American Generator Forum (NAGF), and PSEG expressed concerns with at least some of the disclosure proposed in the First Joint White Paper.

[8] Wolverine Power Comments at 1; ISO-RTO Council Comments at 4; NAGF Comments at 1; Joint Trades Associations Comments at 8-10; MISO TOs Comments at 7; MISO Comments at 3; PSEG Comments at 3; Cogentrix Comments at 2; Memphis Light, Gas and Water Division (MLGW) Comments at 1; and the US Department of Energy (DOE) Comments at 3-4.

[9] NYPA Comments at 1; US Chamber of Commerce Comments at 3.

[10] ISO-RTO Council Comments at 4.

[11] *Id.* at 5.

[12] NAGF Comments at 1.

performance of the Bulk-Power System given its "inherently technical and complex nature."[13]

In comments submitted by the U.S. Department of Energy (DOE), the DOE opined that the Commission may not be taking full advantage of its existing and available authority for protecting CEII and other confidential information. To protect against any incidental disclosure of CEII, the DOE asserted that section 215A of the Federal Power Act (FPA) gives the Commission the authority to designate, protect, and share CEII. In response to FOIA requests for CIP noncompliance submissions, DOE recommended protecting the information as CEII (FOIA Exemption 3) and as confidential business information (FOIA Exemption 4). The DOE comments argued that the use of FOIA Exemption 4 is supported by a recent Supreme Court decision that effectively broadens the scope of information eligible for exemption from disclosure under FOIA Exemption 4.[14]

IV. New Format and Treatment of Future CIP Noncompliance Filings and Submittals

As discussed below, based on a review of the comments, the joint staffs have determined that the First Joint White Paper proposal is insufficient to protect the security of the Bulk-Power System and therefore modify the prior proposal. While the First Joint White Paper proposal sought to strike a balance between security and transparency, the comments demonstrate that the disclosure of CIP noncompliance information risks the security of the Bulk-Power System. Moreover, the First Joint White Paper proposal did not fully avail itself of the Fixing America's Surface Transportation (FAST) Act's CEII protections, nor fully acknowledge relevant Commission precedent providing a greater level of protection for this type of sensitive information.[15] Accordingly, going forward, CIP noncompliance submissions (i.e., NOPs, SNOPs, FFTs, and CEs) will be filed or submitted by NERC with a request that the entire filing or submittal be designated as CEII and Commission staff will designate the entire filing or submittal accordingly. Because of the risk associated with the disclosure of CIP noncompliance information, NERC will no longer publicly post redacted versions of CIP noncompliance filings and submittals.

---

[13] GSOC and GTC Comments at 7.

[14] DOE Comments at 4, 8-9 (*citing Food Mktg. Inst. v. Argus Leader Media*, 139 S.Ct. 2356 (2019).

[15] Order No. 672, 114 FERC ¶ 61,104 at P 538; FAST Act, Pub. L. No. 114-94, § 61,003, 129 Stat. 1312, 1773-1779 (2015) (codified as 16 U.S.C. § 824o-1).

A. Disclosing CIP Noncompliance Information Risks the Security of the Bulk-Power System

The comments demonstrate that under the First Joint White Paper proposal adversaries could still use the limited information proposed for disclosure in CIP noncompliance filings to threaten the reliable operation of the Bulk-Power System.[16] Even the comments supporting additional disclosures acknowledge the ongoing attempts by foreign governments to infiltrate the Bulk-Power System.[17] In addition to foreign governments, hackers and other malicious actors could attempt to exploit vulnerabilities through phishing attacks and data mining using public information in CIP noncompliance filings.[18] Aggressors may try to use data to find a registered entity with weak compliance history with the CIP Reliability Standards and concentrate their efforts on exploiting this weak link.[19] Furthermore, in conjunction with the information revealed in the First Joint White Paper proposal, an aggressor's basic data mining may reveal an entity's location, operating footprint, and facility details—resulting in more serious risks to the Bulk-Power System.[20]

While some commenters assert that releasing the information proposed in the First Joint White Paper would not supply an attacker with actionable information, these commenters do not address the concern that CIP information, when combined with other publicly available information, may help an attacker. Indeed, commenters supporting greater disclosure assert that bad actors may already know much of the information that would be non-public under the First Joint White Paper proposal.[21] That certain sensitive information regarding the security of the Bulk-Power system could be available to bad actors is not a reason for greater disclosure; indeed, greater disclosure could create a forum for bad actors to aggregate and analyze data related to cyber system weaknesses.

While the First Joint White Paper framed the initial proposal as a way of balancing security and transparency concerns, as discussed in the following sections, any treatment of CIP noncompliance must be consistent with the Commission's obligation to protect the

---

[16] Joint Trades Associations Comments at 22; Cogentrix Comments at 2.

[17] Cotter Comments at 3, Attachment; Schleinkofer Comments at 1.

[18] DOE Comments at 6.

[19] *Id.* at 7.

[20] *Id.*

[21] *See* Cotter Comments at 3; Schleinkofer Comments at 1.

security of the Bulk-Power System, notwithstanding the putative benefits of public disclosure raised in the comments.

Even weighing the assumed benefits of public disclosure articulated by commenters, the principal policy reason for such disclosure—incenting compliance with the CIP Reliability Standards—is not compelling because section 215 of the FPA relies primarily on the prospect of substantial penalties to incentivize compliance with NERC Reliability Standards, rather than through public scrutiny.[22] Registered entities face considerable penalties and required mitigation activities to address noncompliance with the CIP Reliability Standards through a process established under section 215(e) of the FPA. After NERC submits a CIP noncompliance filing or submittal for Commission review, only the Commission may initiate a review either on its own motion or by application of the violator; third parties are not permitted to intervene or seek review of CIP noncompliance filings and submittals.[23] Since the public does not have a statutory role in the enforcement of Reliability Standards, public disclosure of CIP noncompliance information does not serve any statutory purpose. Although Commission and NERC staffs recognize the potential deterrent effect of publicizing the identity of violators in general, the security concerns discussed here outweigh the potential benefit.

B. New CIP Noncompliance Filing and Submittal Process is Consistent with Commission Precedent

As a number of commenters point out, the Commission determined in Order No. 672 that disclosing the names of violators in CIP NOPs or the disposition of a violation or alleged violation that relates to a Cybersecurity Incident poses a risk to the Bulk-Power System.[24] In Order No. 672, the Commission implemented section 215(e) of the FPA by

---

[22] *See EPIC v. DHS*, 777 F.3d 518, 526-27 (D.C. Cir. 2015), *cert. denied* 136 S.Ct. 876 (U.S. Jan. 11, 2016) (No. 15-196) (finding that even when certain information protected by FOIA "is a matter of significant public interest, balancing when the value of producing certain categories of documents outweighs the government's generic justification for non-disclosure is what the Congress has done in enacting and amending FOIA.").

[23] Third parties may only take part in Commission reviews of NOPs after the Commission has formally determined to review the NOP. Even then, section 39.7(e)(7) of the Commission's regulations provide that the Commission may find that "a nonpublic proceeding is necessary and lawful, including a proceeding involving a Cybersecurity Incident."

[24] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability*

promulgating section 39.7(b)(4) of the Commission's regulations, which addresses the public treatment of noncompliance submissions before and after NERC files them with the Commission:

> Each violation or alleged violation shall be treated as nonpublic until the matter is filed with the Commission as a notice of penalty … [however, the] disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk-Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise.

In Order No. 672, the Commission explained that:

> 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 … 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 Commission proceedings … the benefits of transparency are overridden in the limited situation of cases in which such transparency would jeopardize Bulk-Power System security.[25]

Maintaining the confidentiality of CIP NOPs in their entirety is consistent with the Commission's reasoning in Order No. 672. While CIP noncompliance filings and submittals do not necessarily involve Cybersecurity Incidents (i.e., "a malicious act or suspicious event"), section 39.7(b)(4) of the Commission's regulations also recognizes the need to preserve confidentiality as it pertains to "[t]he disposition of each violation or alleged violation … that would jeopardize the security of the Bulk-Power System if publicly disclosed." As discussed in the prior section, the comments support the conclusion that disclosing information in CIP noncompliance filings and submittals jeopardizes the security of the Bulk-Power System. Accordingly, designating CIP

Standards, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

[25] Order No. 672, 114 FERC ¶ 61,104 at PP 535, 538.

noncompliance filings and submittals as nonpublic in their entirety is consistent with Order No. 672.

C. The New Filing and Submittal Process Protecting CIP Noncompliance Filings is Consistent with the Application of Various FOIA Exemptions and the FAST Act.

As discussed below, the joint staffs believe that withholding CIP noncompliance filings and submittals in their entirety is justified under FOIA Exemptions 3, 4, and 7(F) and the FAST Act.

Under FOIA Exemption 3, the disclosure of records that are "specifically exempted from disclosure by statute" is prohibited if the statute "requires that the matters be withheld from the public in such a matter as to leave no discretion on the issue; or … establishes particular criteria for withholding or refers to particular types of matters to be withheld[.]"[26] The FAST Act includes such an express requirement that the Commission not disclose information that it designates as CEII.[27]

The FAST Act defines "critical electric infrastructure information"[28] as:

> Information *related to* critical electric infrastructure, or proposed critical electric infrastructure, generated by or provided to the Commission…other than classified national security information, *that is designated as critical electric infrastructure information by the Commission* or the Secretary pursuant to subsection (d). Such term includes information that qualifies as critical energy infrastructure information under the Commission's regulations.[29]

Applying this definition, CIP noncompliance filings and submittals fall within the scope of critical electric infrastructure information. As comments illustrate, even information such as the penalty amount, when coupled with information on the standard

---

[26] 5 U.S.C. § 552(b)(3) (2018).

[27] 16 U.S.C. § 824o-1(d)(1).

[28] The FAST Act defines "critical electric infrastructure" as "a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters." 16 U.S.C. § 824o-1(a)(2).

[29] 16 U.S.C. § 824o-1 (emphasis added).

violated or an entity's name, may provide information on the magnitude of the violation in relation to critical electric infrastructure.[30] Having determined that the public disclosure of CIP noncompliance filings and submittals poses a risk to the reliable operation of the Bulk-Power System, CIP noncompliance filings and submittals will be designated CEII. CIP noncompliance filings are provided to the Commission to impose penalties on users, owners and operators of the Bulk-Power System for violating CIP Reliability Standards pursuant to section 215(e) of the FPA. CIP Reliability Standard violations necessarily involve Bulk-Power System facilities, and these facilities qualify as "critical electric infrastructure" because their incapacity or destruction "would negatively affect national security, economic security, public health or safety, or any combination of such matters."[31] Accordingly, pursuant to the express language of the FAST Act, Commission staff will not disclose CIP noncompliance filings and submittals in response to FOIA requests because they consist entirely of CEII.

In addition, FOIA Exemption 4 protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."[32] CIP noncompliance submissions meet the legal definition of "commercial information," as construed by the courts, because the disclosure of CIP Reliability Standard violations could materially affect the financial well-being of the registered entity and therefore its ability to provide safe and reliable service.[33] In addition, CIP noncompliance submissions qualify as "privileged or confidential" information. CIP noncompliance information is filed or submitted by NERC, a non-government entity not subject to FOIA, and contain information provided, in part, from registered entities.[34] As discussed in the DOE comments, the Supreme Court held in *Food Marketing Institute v. Argus Leader Media* that "information communicated to another remains confidential whenever it is

---

[30] *See e.g.*, Joint Trades Associations Comments at 14.

[31] 16 U.S.C. § 824o-1(a)(2).

[32] 5 U.S.C. § 552(b)(4).

[33] *See Critical Mass Energy Project v. Nuclear Energy Commission*, 830 F.2d 278, 281 (D.C. Cir. 1987), *vacated en banc on other grounds*, 975 F.2d 871, 880 (D.C. Cir. 1992).

[34] "Information is considered 'obtained from a person' [under Exemption 4] if the information originated from an individual, corporation, or other entity, and so long as the information did not originate with the federal government." *EPIC v. DHS*, 117 F. Supp. 3d 46 (D.D.C. 2015) (*citing Bd. of Trade of City of Chicago v. Commodity Futures Trading Commission*, 627 F.2d 392, 404 (D.C. Cir. 1980)).

customarily kept private, or at least closely held, by the person imparting it."[35] The Court also suggested that there must also be an express or implied promise from the government to maintain its secrecy or confidentiality.[36] CIP noncompliance submissions may therefore be protected under Exemption 4 if: (1) the information has been maintained by the submitters as confidential; and (2) the Commission has provided an assurance of confidentiality.[37] Here, Commission staff has determined that it will maintain the confidential treatment of CIP noncompliance information in line with the FAST Act, FOIA exemptions, and applicable case law.

Finally, FOIA Exemption 7(F) protects law enforcement information where its release "could reasonably be expected to endanger the life or physical safety of any individual."[38] This exemption has been successfully applied in cases involving information like that contained in the CIP noncompliance submissions.[39] For example, courts have been generally deferential when it comes to assessing national security harms when an agency determines there is a reasonable expectation of danger.[40] In cases

---

[35] *See* DOE Comments at 8 (*citing Food Mktg. Inst. v. Argus Leader Media*, No. 18-481, 139 S.Ct. 2356 (2019).

[36] *EPIC v. DHS, supra* n.34.

[37] Following the Court's issuance of *Argus*, the Department of Justice issued guidance for agencies opining that an "express assurance" of confidentiality can be made by: direct communications with the submitter; general notices on agency websites; or through regulations indicating that information will not be publicly disclosed. *See "*OIP Guidance: Exemption 4 after the Supreme Court's Ruling in *Food Marketing Institute v. Argus Leader Media*" (Oct. 3, 2019).

[38] *See* 5 U.S.C. § 552(b)(7)(F).

[39] *See Public Employees for Environmental Responsibility* v. *U.S. Section, Int'l Boundary and Water Com'n, US-Mexico,* 740 F.3d 195, 205-206 (D.C. Cir. 2014) ("The inundation maps fall within Exemption 7(F)."); *Greenpeace, Inc.* v. *Dep 't of Homeland Security,* 311 F. Supp. 3d 110, 129 (D.D.C. 2018) (granting motion for summary judgment in favor of DHS as to assertion of Exemption 7(F) as to the identity of the "tiered" and "detiered" chemical facilities under CFATS."). Courts have also found that the exemption applies in situations in which the "individual" who may be endangered cannot necessarily be identified in advance. *See EPIC* v. *DHS,* 777 F.3d 518, 524 (D.C. Cir. 2015) ("The language of Exemption 7(F), which concerns danger to the life or physical safety of any individual, suggests Congress contemplated protection *beyond a particular individual who could be identified before the fact.*") (emphasis added).

[40] *See id.* (noting Exemption 7(F)'s expansive text and the generally deferential posture courts take when it comes to assessing national security harms) (quotations and

involving documents relating to critical infrastructure, courts have deferred to agency assessments that disclosure may endanger the life or physical safety of any individual.[41] The joint staffs conclude that disclosure of CIP noncompliance information would endanger the reliable operation of the Bulk-Power System by making it more vulnerable to a successful cyberattack, and thereby "could reasonably be expected to endanger the life or physical safety of any individual."[42]

V. Conclusion

As identified by various commenters, there are substantial risks to the security of the Bulk-Power System resulting from the disclosure of CIP violator names and other information found in CIP noncompliance submissions. The joint staffs conclude that the proposal in the First Joint White Paper is insufficient to protect the security of the Bulk-Power System and does not fully implement the Commission's legal authority to shield such information from public disclosure. Accordingly, going forward, NERC will file or submit CIP noncompliance information with a request that the entire filing or submittal be treated as CEII. Commission staff will maintain the confidentiality of those filings and submittals by designating them as CEII in their entirety. Similarly, because of the risk associated with the disclosure of CIP noncompliance information, NERC will no longer publicly post redacted versions of CIP noncompliance filings and submittals.

---

citations omitted); s*ee also Pinson v. DOJ,* 2019 WL 4142165, *10 (D.D.C. Aug. 30, 2019) ("The Court finds that there is a reasonable expectation of danger and defers to [the agency's] expertise in assessing the possible danger.")

[41] *See*, *e.g.*, *Public Employees for Environmental Responsibility,* 740 F.3d at 205-206 ("[In] ... cases involving documents relating to critical infrastructure, it is not difficult to show that disclosure may endanger the life or physical safety of any individual.").

[42] *Id*.

Document Content(s)