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

NOTICE OF WHITE PAPER

(August 27, 2019)

Take notice that the Commission staff is publishing a White Paper prepared jointly with staff from the North American Electric Reliability Corporation (NERC). The White Paper sets out a proposed new format for NERC Notices of Penalty involving violations of Critical Infrastructure Protection Reliability Standards.[1]

The White Paper is being placed in the record of this administrative docket, referenced above. The White Paper will also be available on the Commission's website at http://www.ferc.gov.

Comments on the White Paper should be filed within 30 days of the issuance of this Notice. The Commission encourages electronic submission of comments in lieu of paper using the "eFiling" link at http://www.ferc.gov. Persons unable to file electronically should submit an original of the comment to the Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426.

All filings in this docket are accessible on-line at http://www.ferc.gov, using the "eLibrary" link. There is an "eSubscription" link on the web site that enables subscribers to receive email notification when a document is added to a subscribed

[1] 16 U.S.C. § 824o(e)(2) (2012).

docket. For assistance with any FERC Online service, please email FERCOnlineSupport@ferc.gov, or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Questions regarding this Notice should be directed to:

Jonathan First
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-8529
Jonathan.First@ferc.gov

Kimberly D. Bose,
Secretary.

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

DOCKET NO. AD19-18-000

AUGUST 27, 2019

FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILTY 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

This joint White Paper prepared by the staffs of the Federal Energy Regulatory Commission (Commission) and the North American Electric Reliability Corporation (NERC), addresses NERC's submission, and the Commission's processing, of Notices of Penalty (NOPs) for violations of Critical Infrastructure Protection (CIP) Reliability Standards, which contain requirements that provide for the cybersecurity of the Bulk-Power System. CIP NOPs, as submitted to the Commission 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[1] and/or 18 CFR § 39.7(b)(4), which provides that "[t]he 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" (emphasis added). As a result, 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 the Commission's rules and regulations.

The Commission'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 Commission staff finds that the information is not entitled to such treatment.[2] Commission staff does not make determinations on NERC's requests for CEII designation at the time of filing; however, the information is maintained as non-

[1] *See* 18 C.F.R. § 388.113 (2018). CEII or information that would otherwise pose a risk to the security of a NERC registered entity are exempt from public disclosure under the Freedom of Information Act (FOIA) Exemptions 3 and 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (2012) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."); *see also* the Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)).

[2] *See id*. § 388.113(d)(1)(iv) (stating that by maintaining the information as non-public, "the Commission is not making a determination on any claim of CEII status"); *see also Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information; Availability of Certain North American Electric Reliability Corporation Databases to the Commission*, Order No. 833, 157 FERC ¶ 61,123, at P 48 (2016), *order on clarification and reh'g*, Order No. 833-A, 163 FERC ¶ 61,125 (2018).

public in the Commission's filing system, eLibrary, until such time as Commission staff determines that it is not entitled to CEII treatment (e.g., in response to a third-party information requests).[3] While NERC has submitted CIP NOPs containing CEII requests since 2010, Commission staff did not assess a NERC request for CEII designation until 2018 when, for the first time, the Commission received a FOIA request seeking the name of an undisclosed CIP violator (referred to by NERC as an "unidentified registered entity" or "URE").[4]

The Commission has recently received an unprecedented number of FOIA requests for non-public information in CIP NOPs. Consistent with its regulations, Commission staff has released the identity of UREs 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. The significant increase in FOIA requests for non-public information in CIP NOPs has raised security and transparency concerns within industry and the general public, which has prompted Commission and NERC staffs to re-evaluate the format of CIP NOPs filed with the Commission. The current filing format, containing detailed violation information, when coupled with the potential release of URE identities, may not be achieving an appropriate balance of security and transparency. To that end, this White Paper proposes a revised format that is intended to improve this balance.

Specifically, under the proposal, NERC CIP NOP submissions would consist of a proposed public cover letter that discloses the name of the violator, the Reliability Standard(s) violated (but not the Requirement), and the penalty amount. NERC would submit the remainder of the CIP NOP filing containing details on the nature of the violation, mitigation activity, and potential vulnerabilities to cyber systems as a non-public attachment, along with a request for the designation of such information as CEII. This proposal would allow for transparency related to the identity of the entity and violation while protecting the more sensitive security information that could jeopardize the security of the Bulk-Power System. The proposal would only apply to future CIP NOPs submitted by NERC,[5] and it would not affect CIP NOPs already filed with the

[3] Pursuant to the Commission's regulations, the Commission's CEII Coordinator determines whether information should be designated as CEII. The CEII Coordinator makes his determination after consultation with the relevant technical staff.

[4] 5 U.S.C. § 552; 18 C.F.R. § 388.108.

[5] As well as future Spreadsheet NOPs, Find, Fix, Track, and Report issues, and Compliance Exceptions.

Commission. Nor does the proposal affect pending FOIA requests pertaining to previously-filed CIP NOPs.

Commission and NERC staffs believe that the proposed revised format appropriately balances security and transparency concerns. The proposal provides a straightforward format for separating public and non-public information that should achieve efficiencies in submission and processing of CIP NOPs, and lessen the potential for inadvertent disclosure of non-public information. While names of violators would be made public with each CIP NOP submission, detailed information that could be useful to a person planning an attack on critical infrastructure, such as details regarding violations, mitigation and vulnerabilities, would likely be considered by Commission staff to be exempt from FOIA. Thus, as explained below, the revised approach would better protect the electric grid by making less sensitive information available to potential bad actors. Moreover, the proposal segregates information between the public cover letter and non-public attachment in a manner that is consistent with relevant law, including section 215 of the Federal Power Act (FPA), the Fixing America's Surface Transportation Act (FAST Act) and FOIA.[6]

As set forth in the notice being issued contemporaneously with this White Paper, Commission and NERC staffs seek comment on this proposal. In particular, we seek comment on the following:

- The potential security benefits from the new proposed format;
- Any potential security concerns that could arise from the new format;
- Any other implementation difficulties or concerns that should be considered.
- Whether the proposed format provide sufficient transparency to the public.

Moreover, commenters may offer other suggested approaches to the format of CIP NOPs that address the need to protect sensitive information that could be useful to a person planning an attack on critical infrastructure while balancing the goals of transparency and efficiency.

The Commission and NERC are not making any changes to the CIP NOP filing format at this time. Rather, any changes will occur after consideration of public comment on the White Paper.

[6] 16 U.S.C. § 824o (2012); Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61,003, 129 Stat. 1312, 1773-1779 (2015) (codified at 16 U.S.C. § 824o-1).

II. Background

A. FPA Section 215(e) and related Commission regulations

Pursuant to section 215(c) of the FPA, the Commission certified NERC as the electric reliability organization (ERO) with responsibility for developing and enforcing mandatory Reliability Standards.[7] Section 215(e) of the FPA authorizes NERC as the ERO to impose a penalty on a user, owner, or operator of the Bulk-Power System for violation of a Commission-approved Reliability Standard.[8] For a NERC-imposed penalty to take effect, NERC must submit an NOP, including the record of the proceeding, to the Commission. The entity that is the subject of the violation has 30 days to seek review of the penalty, or the Commission may review the penalty on its own motion. If no review is sought, the penalty takes effect on the 31st day after NERC's filing.

In Order No. 672, the Commission promulgated regulations to implement section 215(e) of the FPA.[9] The Commission's regulations address the treatment of CIP NOPs before they are filed with the Commission, after they are filed with the Commission and when the Commission determines to review a CIP NOP. In particular, Section 39.7(b)(4) of the Commission's regulations addresses the public treatment of NOPs before and after they are filed 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.

Section 39.7(e)(7) of the Commission's regulations governs the confidentiality afforded CIP NOPs *after* the Commission institutes a proceeding to review it, either on

---

[7] 16 U.S.C. § 824o(c).

[8] *Id.* § 824o(e).

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

the Commission's own motion or because the violator has made application for review:

> A proceeding for Commission review of a penalty for violation of a Reliability Standard will be public unless the Commission determines that a non-public proceeding is necessary and lawful, including a proceeding involving a Cybersecurity Incident.[10]

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.[11]

While allowing for the possibility of a non-public proceeding involving a CIP NOP, the Commission indicated that these provisions in sections 39.7(b)(4) and 39.7(e)(7) pertain to limited situations involving a Cybersecurity Incident or other matters that would jeopardize Bulk-Power System security if publicly disclosed.[12]

---

[10] 18 C.F.R. § 39.7(e)(7).

[11] Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 535 and 538; *see also id.* P 540 (noting that the Commission determines on a case-by-case basis whether a particular NOP review proceeding "can and should be nonpublic"). Order No. 672 does not address the interplay between the section 39.7 regulation and FOIA.

[12] FPA section 215(a) defines Cybersecurity Incident as "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."

B. FAST Act, CEII and FOIA

1. FAST Act and CEII

In 2016, the Commission amended its CEII regulations to implement the FAST Act. The amended regulations require that a submitter's justification for CEII treatment "must provide how the information, or any portion of the information, qualifies as CEII as the terms are defined in paragraphs (c)(1) and (2) of this section."[13] The amended regulations also require submitters to "include a clear statement of the date the information was submitted to the Commission, how long the CEII designation should apply to the information and support for the period proposed."[14] The amended regulations further warn that "[f]ailure to provide the justification or other required information could result in denial of the designation and release of the information to the public."[15]

The amended regulations state that, "documents for which privileged treatment is claimed will be maintained in the Commission's document repositories as non-public until such time as the Commission may determine that the document is not entitled to the treatment sought."[16] The amended regulations also make clear that, "by treating the documents as nonpublic, the Commission is not making a determination on any claim of privilege status and [it] retains the right to make determinations with regard to any claim of privilege status, and the discretion to release information as necessary to carry out its jurisdictional responsibilities."[17]

---

[13] 18 C.F.R. § 388.113(d)(1)(i).

[14] *Id.*

[15] *Id.*

[16] 18 C.F.R. § 388.112(c)(1)(i); *see also* 18 C.F.R. § 388.113(d)(1)(iv) ("information for which CEII treatment is claimed will be maintained in the Commission's files as non-public until such time as the Commission may determine that the information is not entitled to the treatment sought … [b]y treating the information as CEII, the Commission is not making a determination on any claim of CEII status").

[17] 18 C.F.R. § 388.112(c)(1)(i).

2. FOIA

Pursuant to FOIA, any person has the right to request public access to federal agency records. The Commission's Office of External Affairs (OEA) is the lead office within the Commission for handling FOIA requests, and the Director of OEA is responsible for making FOIA determinations.

Under FOIA, the Commission must release records upon receiving a written request unless the records fall within one or more of nine exemptions and three exclusions outlined in the Act. In the context of FOIA requests seeking information on a CIP-related Notice of Penalty, potential exemptions which may apply include, but are not limited to, FOIA Exemption 3. Exemption 3 incorporates into FOIA certain nondisclosure provisions that are contained in federal statutes. *See* 5 U.S.C. 552(b)(3). CEII is specifically exempt from disclosure under the FAST Act. To avoid disclosure under FOIA, one of the clearly-defined exemptions in the statute must apply.

C. **Description of CIP NOP submissions from 2010-2019**

The Commission approved the Version 1 CIP Reliability Standards on January 18, 2008.[18] On July 6, 2010, NERC made its first CIP NOP filing, which included public and non-public versions. NERC requested designation of the name of the violator as CEII, referring to the violator as a URE in the public filing. With only one exception, NERC has sought CEII treatment for the name of the violator in all CIP NOPs.[19]

From July 2010 until December 2018, the public version of the CIP NOPs was not a redacted version of the confidential filing. Rather, the public CIP NOP submission contained similar information as the confidential submission without the material that NERC believed constituted CEII, including the name of the URE. To better conform to the Commission's regulations, NERC changed this format in 2019, showing in the public version of CIP NOPs line-by-line redactions of information claimed as CEII in the

[18] *See Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040 (2008), Order No. 706-A, 123 FERC ¶ 61,174 (2008), Order No. 706-B, 126 FERC ¶ 61,229 (2009), and Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[19] In Docket No. NP11-238-000, the CIP NOP identified the Southwestern Power Administration, a federal power marketer, as the violator. The identity of the entity in this particular case was material to the resolution of the matter, as the entity had asserted a defense regarding the extent of the Commission's authority to impose a monetary penalty on a federal entity.

confidential versions, including redacting the identity of the URE.[20]

III. Proposed Revisions to the Format for the Future Submission of CIP NOPs and Assertions of CEII.

A. Reason for proposed revisions to CIP NOP format

Commission and NERC staffs believe that certain revisions to the format of CIP NOPs will have multiple benefits, including ensuring a better security posture with regard to the public dissemination of potentially sensitive information, closer adherence to the requirements of the Commission's CEII regulations, and greater efficiency in the submission and processing of CIP NOPs. This White Paper is not proposing any changes to the Commission's rules governing the submission of NOPs (18 C.F.R. § 39.7(b)(4)) or the Commission's CEII rules and regulations (18 C.F.R. § 388.113).

As discussed above, NERC began submitting CIP NOPs in July 2010; and since that time, NERC's submissions have included requests that the Commission designate certain information contained therein, including the violator's name, as CEII.

Commission staff did not immediately make a determination on NERC's request for CEII designations.[21] Consistent with Commission regulations, the Commission staff maintained the information as non-public in the Commission filing system, eLibrary.[22] In 2018, for the first time, the Commission received a FOIA request seeking the name of a URE, which then required Commission staff to make a CEII determination. Since that time, the Commission has received multiple FOIA requests seeking the identities of UREs, as well as other CIP NOP information for which NERC has requested a CEII designation.

Consistent with the Commission's CEII and FOIA rules and regulations, Commission staff engages in a case-by-case review of each CIP NOP subject to a FOIA request to determine whether URE identity and other information is protectable under FOIA. Under its current process, the publicly available information of each CIP NOP

[20] *See* 18 C.F.R. § 388.113(d)(1) (stating that a person requesting that information be treated as CEII must also submit a public version "where CEII is redacted, to the extent practicable").

[21] Pursuant to the Commission's regulations, the Commission's CEII Coordinator determines whether information should be designated as CEII and thus withheld under FOIA.

[22] 18 C.F.R. 388.113(d)(1)(iv).

submitted by NERC typically includes details regarding the underlying violations, mitigation measures, and possibly other significant details about cyber assets and operating systems. Thus, Commission staff's evaluation of whether to release non-public CIP NOP information turns on whether the information, such as the name of the URE, coupled with the public information normally contained in CIP NOPs, would reasonably provide useful information to a person planning an attack on critical infrastructure. In such instances, when Commission staff has determined that the release would provide useful information to a person planning an attack, staff has designated the information as CEII and withheld the identity of the URE under FOIA. However, in those instances where Commission staff determines that releasing non-public CIP would not reasonably provide useful information to a person planning an attack on critical infrastructure, the requested information has been released. An example of this might include the violation of a retired, administrative requirement such as the requirement to generate logs of adequate detail for audit purposes.

Recent FOIA requests seeking the names of CIP violators have resulted in the release of the CIP violator's identity in limited instances. As noted previously, security and transparency concerns within industry and the general public have prompted the Commission and NERC staffs to re-evaluate whether NERC should publically identify certain basic pieces of information in CIP NOPs that, in themselves, likely do not pose a security risk (i.e., the name of the violator, the Reliability Standard(s) violated and the penalty amount) and seek designation of the details of the violations as confidential. As discussed below, the proposed revised format would make such information publicly available while at the same time preserving NERC's ability to seek CEII treatment for information more likely to pose security risks (i.e., nature of the violation, mitigation activity, and potential vulnerabilities to cyber systems) in order to achieve an appropriate balance of security and transparency.

B. Structure of the revised CIP NOP submission format

This White Paper proposes a new approach in which NERC would submit CIP NOPs containing a public cover letter and a confidential attachment. The cover letter would publically disclose:

(1) the name of the violator,

(2) the Reliability Standard(s) violated (but not the requirement or sub-requirement violated), and

(3) the penalty amount.

NERC would provide details on the nature of the violation, mitigation activity, and potential vulnerabilities to cyber systems in a confidential attachment. The proposed

cover letter would also contain a request for designation of the confidential attachment as CEII, as well as relevant, non-substantive information such as the Regional Entities involved in the compliance matter.

Moreover, under this proposal, NERC would submit CIP NOPs only after mitigation of the underlying violation is completed. This will further minimize the possibility of any adversarial insight resulting from the disclosure of violator names, nor should it materially delay CIP NOP filings.[23] If implementation of the proposal exposed problems, this facet of the proposal could be revisited. This proposal would apply to "Full" CIP NOPs as well as to the less formal spreadsheet NOPs; "find, fix, track, and report" noncompliance postings, and compliance exceptions.

Finally, while the proposed CIP NOP submission format described above should apply in most, if not all circumstances, a situation could occur in which the identification of the violator's name might justifiably be designated as CEII.[24] In such a circumstance, NERC would still have the ability to seek CEII treatment for the name of the violator pursuant to the Commission's regulations.

The public identification of the CIP violator may result in increased hacker activity such as scanning of cyber systems and possible phishing attempts. However, the joint staffs believe that the limited information provided in the proposed cover letter would not provide an adversary with insights on the nature of the CIP violation or related cyber vulnerabilities, processes or procedures that could be used for an informed, focused attack on the violator's cyber assets.

C. Benefits of the revised CIP NOP submission format

Recognizing the strong public interest in the outcome of FOIA requests seeking the identities of UREs in CIP NOPs, Commission and NERC staffs believe that the proposed revised format more appropriately balances confidentiality, transparency, security and efficiency concerns. While names of violators would be made public with each CIP NOP submission, detailed information that could be useful to a person planning an attack on critical infrastructure, such as details regarding violations, cyber-related processes and procedures, mitigation and vulnerabilities, would more clearly fall within the scope of information that is likely to be considered by Commission staff to be exempt

[23] Because most violations are fully mitigated before submission of the NOP, we do not expect a backlog to result.

[24] *See, e.g.,* Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 538 (such designations would be in "limited circumstances" and most likely involve an actual Cybersecurity Incident).

from FOIA. Thus, the new approach would better protect the electric grid by making less information available to bad actors while providing transparency.

The proposal provides efficiencies because the information that would be made available to the public is readily identified and set forth in a cover letter. Perhaps more significantly, there is less opportunity for errors, including the inadvertent disclosure of potential CEII in the preparation and submission of CIP NOPs with line-by-line redactions. Further, under the current approach in which NOPs are submitted masking the name of the violator and providing details of the violation, there is a risk that the name of the violator may become known to the public through inadvertent or intentional disclosure by employees or contractors, or through deduction based on seemingly insignificant details set forth in the NOP. This information, in combination with the details of the violation, could jeopardize the security of the Bulk-Power System. The proposed approach would minimize, if not eliminate, such risk.

Further, the proposed format of the submission of public and non-public CIP NOP information is consistent with relevant law, including section 215 of the FPA, FAST Act and FOIA. Publicly identifying the entity that is the subject of a CIP NOP, as well as the penalty amount and relevant Reliability Standard(s), provides greater transparency regarding reliability compliance, and is consistent with the types of information sought by persons that have submitted FOIA requests regarding CIP NOPs. In addition, the segregation of CEII containing substantive details of CIP violations, mitigations and potential cyber security vulnerabilities is consistent with the process and protections set forth in the FAST Act, as implemented in Part 388 of the Commission's regulations. Thus, the proposal strikes a reasonable balance because it allows for an appropriate level of transparency while providing a sound approach to secure information that could jeopardize the security of the Bulk-Power System. In addition, FERC and NERC will continue to work to ensure lessons learned from all violations remain available to industry.

The joint staffs seek comment on the proposal set forth in this White Paper. In particular, we seek comment on the following:

- The potential security benefits from the new proposed format;
- Any potential security concerns that could arise from the new format;
- Any other implementation difficulties or concerns that should be considered.
- Does the proposed format provide sufficient transparency to the public.

Moreover, commenters may offer other suggested approaches to the format of CIP NOPs that address the need to protect sensitive information that could be useful to a

person planning an attack on critical infrastructure while balancing the goals of transparency and efficiency.

Document Content(s)