UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Security Incident Reporting	**)**	**Docket No. RM18-2-000**
Reliability Standards	**)**	

ANNUAL REPORT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON CYBER SECURITY INCIDENTS

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 21, 2022

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Security Incident Reporting Reliability Standards	**)** **)**	**Docket No. RM18-2-000**

ANNUAL REPORT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON CYBER SECURITY INCIDENTS

Pursuant to paragraph 90 of Order No. 848,[1] the North American Electric Reliability Corporation ("NERC")[2] hereby submits to the Federal Energy Regulatory Commission ("FERC" or the "Commission") the Annual Report on Cyber Security Incidents.[3] Specifically, this report covers the Cyber Security Incidents, including those deemed Reportable Cyber Security Incidents and attempts to compromise applicable systems, received by the Electricity Information Sharing and Analysis Center ("E-ISAC") between January 1 to December 31, 2021 pursuant to Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning.

This report is organized as follows: Section I describes Order No. 848 and FERC approval of CIP-008-6. Section II describes how E-ISAC collects reports. Section III provides the number of the reports received and a request for Critical Energy/Electric Infrastructure Information ("CEII") treatment of information in the Appendix. Section IV includes analysis and next steps. Finally, Section V provides a conclusion to this informational filing.

---

1 *Cyber Security Incident Reporting Reliability Standards*, Order No. 848, 164 FERC ¶ 61,033 (2018) [hereinafter Order No. 848].

2 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

3 Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, https://www.nerc.com/files/Glossary_of_Terms.pdf.

I. BACKGROUND

On July 19, 2018, the Commission issued Order No. 848 directing NERC to develop and submit modifications to the NERC Reliability Standards to augment mandatory reporting of Cyber Security Incidents.[4] Specifically, the Commission directed that NERC modify CIP-008-5 to:

- expand mandatory reporting of Cyber Security Incidents to include compromises of, or attempts to compromise, a Responsible Entity's Electronic Security Perimeter and associated Electronic Access Control or Monitoring Systems ("EACMS") performing certain functions;
- require certain attributes in the incident reports;
- include timelines for submitting the incident reports based on the severity of the incident; and
- require incident reports be submitted to the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"), or its successor, in addition to the E-ISAC.[5]

As mentioned above, the Commission directed that NERC require that the incident reports include the following minimum set of attributes: "(1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident."[6] The Commission also directed NERC to develop reporting timelines that consider the severity of the event and the risk

4 Order No. 848 at P 16.
5 *Id.*
6 *Id.* at P 91.

to Bulk Electric System ("BES") reliability.[7] Finally, the Commission directed NERC to submit an annual anonymized, public summary of the reports.[8]

Consistent with Order No. 848, NERC submitted Reliability Standard CIP-008-6 for FERC approval on March 7, 2019.[9] The Commission approved Reliability Standard CIP-008-6 on June 20, 2019.[10] Effective in the United States on January 1, 2021, Reliability Standard CIP-008-6 specifies processes and procedures to be included in Cyber Security Incident response plans, implementation and testing of these plans, maintenance of these plans, and mandatory reporting on certain Cyber Security Incidents to facilitate information sharing on threats among relevant entities. Requirement R4 of Reliability Standard CIP-008-6 requires Responsible Entities[11] to report Reportable Cyber Security Incidents and attempts to compromise applicable systems to the E-ISAC and successor organizations to ICS-CERT, consistent with the directive in Order No. 848. Requirement R4 also includes requirements regarding the timing and content of reports.

This current filing covers the first year of implementation of Reliability Standard CIP-008-6, from January 1, 2021 to December 31, 2021.

II. E-ISAC REPORT COLLECTION

As noted, Responsible Entities must submit incidents that meet CIP-008-6 reporting requirements to the E-ISAC.[12] The E-ISAC is operated by NERC and facilitates information

---

7 *Id.*

8 *Id.* at P 90.

9 *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-008-6*, Docket No. RD19-3-000 (March 7, 2019).

10 *N. Am. Elec. Reliability Corp.*, 167 FERC ¶ 61,230 (2019) (Letter Order).

11 As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entities subject to the CIP Reliability Standards.

12 Responsible Entities also submit reports to the United States Cybersecurity & Infrastructure Security Agency ("CISA"), the successor organization to ICS-CERT and the National Cybersecurity and Communications Integration Center ("NCCIC").

sharing, promotes situational awareness, and provides resources for asset owners and operators to prepare for and reduce cyber and physical security threats.

To submit reports as required by Reliability Standard CIP-008-6, the E-ISAC offers several options for Responsible Entities. For example, reports may be submitted using the NERC EOP-004 reporting form, the DOE OE-417 form, or directly through the E-ISAC portal. All reports must be submitted consistent with the requirements in CIP-008-6.

III. RECEIVED REPORTS AND CEII JUSTIFICATION

Between the dates of January 1, 2021 and December 31, 2021, Responsible Entities submitted two CIP-008-6 reports to the E-ISAC, described in the confidential Appendix. These two reports include attempts to compromise applicable systems but were unsuccessful. NERC requests CUI/CEII/PRIV treatment for the information in the Appendix as non-public and CEII, consistent with the Commission's Order No. 672, Section 388.113 of the Commission's regulations, the FAST Act, and Freedom of Information Act, Exemptions 3 and 4, respectively.[13] The information in the Appendix reflects CEII within the scope of the Commission's rules as it is related to critical electric infrastructure, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters. Specifically, this information qualifies as CEII because it includes specific attack vectors and defensive solutions that could be useful to a person in planning an attack on critical infrastructure. NERC requests this treatment for the information in the Appendix for the duration of five years, beginning from the date of this filing, because of the potential for a threat actor to

[13] *See Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006); 18 C.F.R. § 388.113(e)(1); FAST Act, Pub. L. No. 114-94, § 61,003, 129 Stat. 1312, 1773-1779 (2015) (codified as 16 U.S.C. § 824o-1); 5 U.S.C. §§ 552(b)(3), (b)(4), and (b)(7) (2018).

use this information to inform future attacks on critical infrastructure. NERC further requests the Commission re-designate the information in the Appendix as CEII as appropriate. NERC notes that re-designation of the information in the Appendix in its entirety may be appropriate at the end of the five year period because the information may, in combination with other publicly available information, be sufficient to help an attacker endanger the reliable operation of the Bulk Power System.

IV. ANALYSIS AND NEXT STEPS

NERC is encouraged that there were no reported successful Cyber Security Incidents during the 2021 calendar year and that entities reported these attempts to the E-ISAC. Nevertheless, given it is the first year of implementation of Reliability Standard CIP-008-6 and the pace of cyber security activity in 2021, NERC and the Regional Entities initiated a review to assess Reliability Standard CIP-008-6 and its implementation. While the ERO Enterprise does not always initiate reviews of standards outside the usual periodic review process, the ERO Enterprise determined to understand the context behind the number of reports received.

The CIP-008-6 standard review effort is an ERO Enterprise-wide activity to gain a better understanding of how registered entities fulfill their obligations to categorize Cyber Security Incidents, including attempts to compromise and Reportable Cyber Security Incidents. By engaging with over 25 entities, the review effort also will provide insight into industry's Cyber Security Incident response reporting criteria and processes as required under Requirement R4 of CIP-008-6. This review effort will permit the ERO Enterprise to determine whether further action, such as outreach or revisions to enhance the standards language, is warranted to accurately reflect any attempts on the grid's most critical cyber security infrastructure. In addition, NERC will

closely coordinate any revisions to CIP-008-6 or other follow up actions with any cyber incident reporting requirements resulting from the Strengthening American Cybersecurity Act of 2022.[14]

V. CONCLUSION

NERC requests the Commission accept this informational filing as consistent with the directives from Order No. 848. NERC will provide any relevant follow up information from its standard review effort in the CIP-008-6 Annual Report covering incidents reported during the 2022 calendar year to be filed in the first quarter of 2023. NERC appreciates the Commission's shared commitment to cyber security and information sharing to help prepare industry for potential threats.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 21, 2022

[14] Strengthening American Cybersecurity Act of 2022, S.3600, 117 Cong. (2022).

The information in Appendix A is CEII and

is not included in the public version of this filing.

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in the above-referenced proceeding.

Dated at Washington, D.C. this 21st day of March, 2022.

/s/ Marisa Hecht

Marisa Hecht
Counsel for North American Electric Reliability Corporation