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

Shamai Elstein
Associate General Counsel
Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
shamai.elstein@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 20, 2023

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 2022 Annual Report on Cyber Security Incidents.[3] This report covers the Cyber Security Incidents received by the Electricity Information Sharing and Analysis Center ("E-ISAC") between January 1 to December 31, 2022 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 the E-ISAC collects reports. Section III provides a summary of the reports received. Section IV discusses next steps. 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/pa/Stand/Glossary%20of%20Terms/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, 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 second year of implementation of Reliability Standard CIP-008-6, from January 1, 2022 to December 31, 2022.

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 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. Reports may be submitted using the NERC EOP-004 reporting

---

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 (Mar. 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").

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. SUMMARY OF REPORTS

Between the dates of January 1, 2022 and December 31, 2022, Responsible Entities submitted eight CIP-008-6 reports to the E-ISAC. The distribution of these reports by Regional Entity is as follows: four in WECC, two in MRO, and two in TexasRE. The following is a summary of the reports and key takeaways.

Attack Vector: Of the reported incidents, the most common attack vector was malware (i.e., malicious code, Trojans, and ransomware). There were four such reported incidents. One of these attacks was the use of a Trojan in an attempt to compromise an Interactive Remote Access asset. Another of these incidents only affected a few systems on the entity's corporate IT network and there were no issues identified on the OT Energy Management Systems/Supervisory Control and Data Acquisition ("EMS/SCADA") network. Two of the malware incidents exploited known vulnerabilities to attack EACMS assets. In one of these attacks a Log4j vulnerability was exploited and in the other a Fortinet vulnerability was successfully exploited.

Of the remaining four incidents, two incidents were related to attacks on third-parties that supported Responsible Entities BES Cyber Systems, one incident was a physical attack, and one report did not identify an attack vector. Both of the third-party vendor attacks occurred in the WECC region. One of these attacks was on a vendor who provided backup SCADA monitoring services for two wind facilities. This attack affected the vendor's internal network and caused outages to email, phone, and access to SCADA. The other third party attack was a Distributed Denial of Service ("DDOS") attack on the vendor's ISP, which impacted the performance of third-party forecasts for a Balancing Authority. This particular outage affected the entity's Variable Energy Resource forecast values used by its scheduling department. The physical attack that was

reported was an attempt to remotely open a gate at a medium impact Facility. The attempt failed and the gate did not open. The final incident was of unknown origin but did lead to the loss of EACMS and Physical Access Control Systems ("PACS") visibility. NERC is further investigating this incident.

Functional Impact and Level of Intrusion: None of the reported Cyber Security Incidents or attempts to compromise successfully compromised a BES Cyber Systems or affected reliable operations. The incidents reported in 2022 seem to have targeted specific systems related to cybersecurity defenses and BES monitoring. Two of the eight attacks were successful in compromising Cyber Assets associated with BES Cyber Systems. As noted, one of these attacks managed to cause a loss of visibility to the EACMS and PACS. The exact cause of this loss of visibility is unknown and further follow-up is in the process of being conducted. Another attack was successful in exploiting an EACMS, and the attacker was able to change several firewall rules and create administrator accounts on the affected devices before being detected. This particular attack utilized a known vulnerability to send specially crafted HTTP or HTTPS messages to several firewall devices. The attacker was able to access the configuration files and added several admin accounts, in addition several settings were changed including the disabling of system diagnostics and admin account automatic timeout.

An additional two attacks were successful on third-party vendors and impacted entities to various degrees. However, neither of these attacks led to any operational impacts that affected the reliability of the BPS. Another attempted attack was successful in targeting a corporate IT system, but had no impact on any BES Cyber Systems or Cyber Assets and did not impact operations in any way. The physical security attack was successful in sending a remote command to open a gate, but was ultimately unsuccessful as the gate did not open. Finally, the attack which utilized the

Log4j vulnerability appears to have been intended to find vulnerable VMWare hosts. No penetration of the Electronic Security Perimeter ("ESP") occurred and although the attack attempted to download additional malware, these were blocked by the entity's other security systems. Again there was no reported impact outside of the impacted systems sending the attacker an "awake" message.

Other Key Takeaways: There were no concentrations of attacks in any quarter as they were relatively evenly spread throughout the calendar year. There was also no evidence that any of the reported incidents were coordinated.

IV. NEXT STEPS

NERC is encouraged that there were no operational impacts from the reported incidents during the 2022 calendar year and that entities reported these attempts to the E-ISAC. However, there were several attacks which impacted Cyber Assets associated with BES Cyber Systems, including EACMS and PACS, which highlights the continued need for vigilance.

To enhance the reporting requirements, NERC initiated a standards development project, Project 2022-05 – Modifications to CIP-008 Reporting Threshold, to further enhance the reporting requirements in CIP-008-6. This project resulted from the ERO Enterprise review efforts conducted in 2022 to assess the implementation of CIP-008-6. Project 2022-05 will develop revisions that provide a minimum expectation for reporting attempts to compromise. The Comment and nomination period for the project have concluded and the standards drafting team has convened.

V. CONCLUSION

NERC requests the Commission accept this informational filing as consistent with the directives from Order No. 848. 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

Shamai Elstein
Associate General Counsel
Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
shamai.elstein@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 20, 2023

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 20th day of March, 2023.

/s/ Marisa Hecht

Marisa Hecht
Counsel for North American Electric Reliability Corporation