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

Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 21, 2024

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

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 2023 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, 2023 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 the 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), *order on reh'g & compliance,* 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC,* 564 F.3d 1342 (D.C. Cir. 2009).

[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 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

---

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

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 third year of implementation of Reliability Standard CIP-008-6, from January 1, 2023, to December 31, 2023.

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 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, 2023, and December 31, 2023, Responsible Entities submitted three CIP-008-6 reports to the E-ISAC. The distribution of these reports by Regional

[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").

Entity is as follows: one in NPCC, one in SERC, and one in WECC. The following is a summary of the reports and key takeaways.

Attack Vector: All three reports can be attributed to unique attack vectors and there were no commonalities noted in the tactics, techniques, or procedures. The first incident was attributed to a ransomware attack on a third party supporting a plant maintenance management system. The attack lasted only a few hours; however, the plant maintenance management system was rendered inoperable during that time and site data was compromised. The third-party vendor was required to restore the system to mitigate the attack.

The second incident occurred when a contractor at a power plant accessed the internet from an emissions control system and inadvertently infected the Responsible Entity's IT systems with malware. IT staff were able to isolate the affected servers and there was no impact to reliability functions.

The last incident was a physical and cyber intrusion by a vendor utilized by the Responsible Entity. The vendor accessed the ID badging system and granted access to 19 vendor employees who had not been authorized or cleared for access. The vendor employees had access to high impact BES Cyber Systems and External Routable Connectivity ("ERC") Zones.

Functional Impact and Level of Intrusion: Two of the reported Cyber Security Incidents failed to compromise BES Cyber Systems or affect reliable operations. These incidents impacted secondary systems like maintenance, lockout-tagout, and other corporate IT systems. In addition, both intrusions were identified within hours and mitigated quickly to reduce any impacts these systems might have in reliable operations.

The other attack was more serious in its level of intrusion. The vendor was able to grant access to the ID badging system (cyber intrusion) and grant access to several of its employees to

high impact BES Cyber Systems and ERC Zones (physical intrusion). While there were no functional impacts to the BES Cyber Systems or the reliable operation of the BPS, this incident highlights the importance of monitoring third-party access.

Other Key Takeaways: In 2023, the three reports of Cyber Security Incidents are considered attempts to compromise. There were no Reportable Cyber Security Incidents submitted in 2023. There was an overall reduction in the number of reports from eight to three from 2022 to 2023. It should also be noted that the three 2023 attacks involved contracted employees at the Responsible Entities. This highlights the importance of remaining vigilant not only of systems operated by the Responsible Entities but also of systems maintained or operated by contracted third parties. This is a theme that was present in both 2022 and 2023.

Over the past three years, the E-ISAC has received thirteen reports on Cyber Security Incidents, none of which were Reportable Cyber Security Incidents. **Figure 1** shows the breakdown of Cyber Security Incidents by year. The E-ISAC received the most reports in 2022, which included eight Cyber Security Incidents. Both 2021 and 2023 had fewer overall CIP-008-6 reports, with two Cyber Security Incidents in 2021 and three in 2023. There has generally been no pattern in the time of year when Cyber Security Incidents occur, with no quarter of any year consistently having reports.

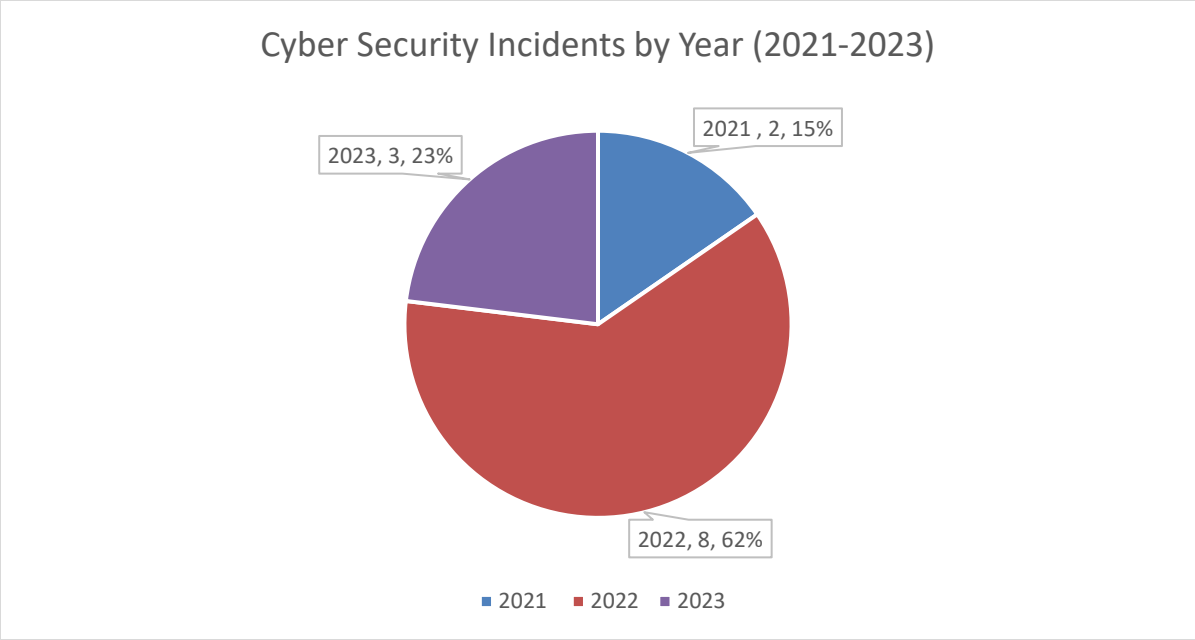

Figure 1. Cyber Security Incidents by Year (2021-2023)

Approximately 50% of the reported Cyber Security Incidents have been attributed to the use of malware as the attack vector. **Figure 2** shows the breakdown of various attack vectors based on the reports received. As noted, the largest share of attack vectors has been malware, followed by two attacks on third-parties who support BES operations, and then brute-force, insider threats, physical security, and the use of TOR Exit Nodes, each attributed to a separate report.

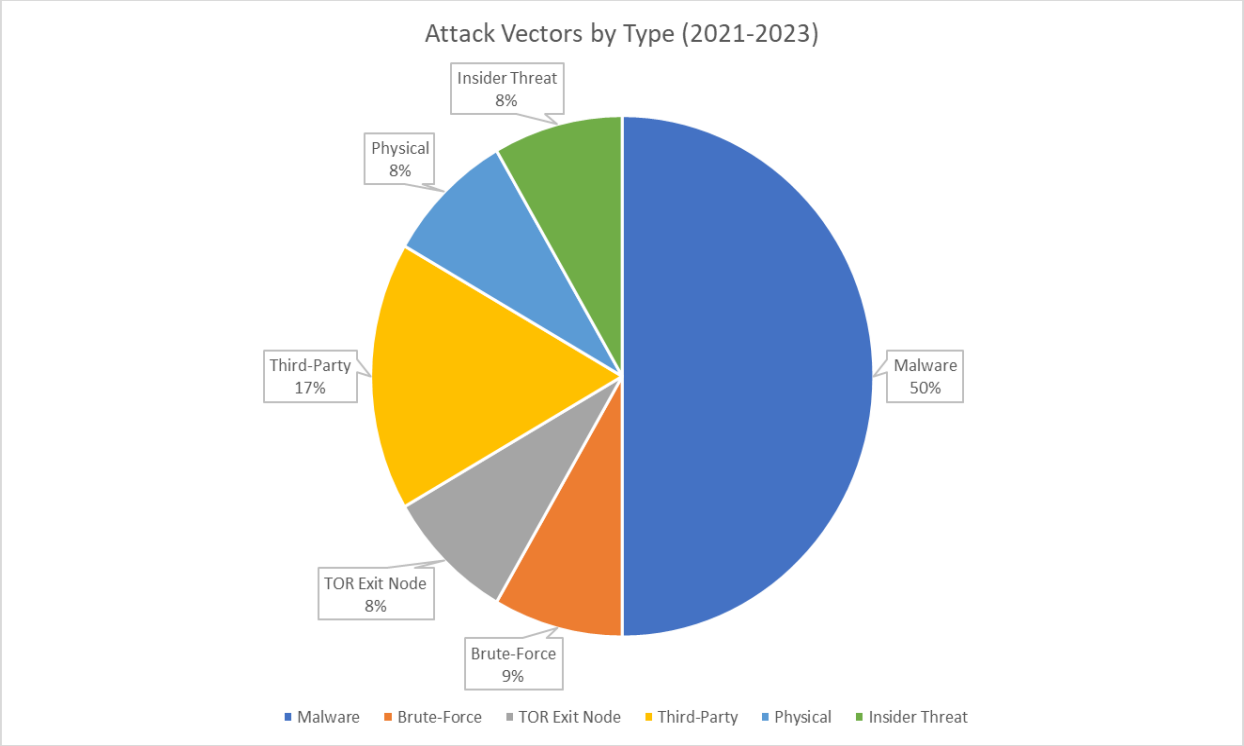

Figure 2. Attack Vectors by Type (2021-2023)

Due to the limited number of reports over the last three years (13), NERC cannot establish attack vector trends. While it appears that malware, such as trojan horses and ransomware, are most common, NERC encourages Responsible Entities to maintain vigilance of other attack vectors as there has not been an established trend at this time based on the reports received in the last three years. As NERC continues its annual analysis of Cyber Security Incidents, NERC will continue to look for trends and include such analysis in future filings.

IV. NEXT STEPS

NERC is encouraged that there were no operational impacts from the reported incidents during the 2023 calendar year and that entities reported these attempts to the E-ISAC. However, each of these Cyber Security Incidents involved either BES Cyber Systems or systems used to support the reliable operation of the BES, 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. The NERC Standards Committee accepted a revised Standard Authorization Request and appointed the Project 2022-05 Drafting Team in July 2023. The Drafting Team is developing revisions to provide a minimum expectation for reporting attempts to compromise.

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

Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410 Washington,
D.C. 20005
(202) 400-3000
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 21, 2024

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, 2024.

/s/ Marisa Hecht

Marisa Hecht
Counsel for North American Electric Reliability Corporation