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, 2025

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 2024 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, 2024 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 fourth year of implementation of Reliability Standard CIP-008-6, from January 1, 2024, to December 31, 2024.

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, 2024, and December 31, 2024, Responsible Entities submitted three CIP-008-6 reports to the E-ISAC, which consisted of Cyber Security Incidents that were attempts to compromise. The distribution of these reports by Regional Entity is as follows:

[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”).

one in NPCC, one in RF, and one in WECC. The following is a summary of the reports and key takeaways. The summary is organized by attributes of received Cyber Security Incidents (attack vector and level of intrusion and functional impact). This summary uses the labels Report A, Report B, and Report C to describe the three reported Cyber Security Incidents to maintain confidentiality and limit release of attributable information.

Attack Vector: Two reports included incidents that targeted Intermediate Systems through failed login attempts. One report included an attempt to scan the network for vulnerabilities. The two attacks that targeted Intermediate Systems through failed login attempts were similar in that they involved multiple Internet Protocol ("IP") addresses. In report B, both of the attempts that were reported were from foreign IP addresses, implying they may have been linked.

Report A consisted of an attempt to compromise that occurred when a Responsible Entity received 20 alerts from its Security Information and Event Monitoring ("SIEM") for failed login attempts to a medium impact BES Cyber System ("BCS") via an Intermediate System. The attempts appear to have originated from two geographically separated IP addresses (Wyoming and Florida). Both IP addresses used the same username for the attempt, leading the entity to believe it was from the same attacker.

Report B consisted of two attempts to compromise when the entity discovered many failed VPN authentication attempts. The entity submitted one report although the attempts to compromise happened approximately one month apart. The first of these two attempts to compromise was a brute force attack originating from multiple IP addresses from a foreign country. Users were locked out, and the entity noted the IPs were associated with reports related to brute force attacks documented by AbuseIPDB and Talos[13]. The second of these two incidents occurred when the entity received a large volume of failed authentication attempts on the same virtual private network ("VPN") interface as noted in the brute force attack. The attempts reported appear to have originated from multiple IP addresses in multiple countries; however they were all linked by the same internet service provider.

Report C was an attempt to compromise that occurred when a Responsible Entity observed a foreign IP address attempting to perform an active MITRE ATT&CK[14] scan of its SCADA network. Based on a log review, it appears the attacker only made initial connections to the network and then was blocked by the entity's firewall. The attack remains under investigation to determine the source of the attack.

Functional Impact and Level of Intrusion: None of the reported Cyber Security Incidents compromised or functionally impacted BCS nor did they impact BPS reliability. The level of intrusion and impacts are described below.

Report A did not identify any functional impacts and the incident was fairly limited in its scope. The attacker was unable to gain access to the medium impact BCS. The entity did not report any operational impacts, and there was no impact to BPS reliability. The controls in place were effective in identifying and mitigating the attempt to compromise.

Report B noted that the first attempt to compromise (brute force) was successful in locking an unspecified number of user accounts. This attempt to compromise appears to have been less sophisticated, but it may have served as a precursor to the second attempt to compromise detailed

[13] AbuseIPDB and Talos are organizations that provide threat intelligence related to cybersecurity. For example, AbuseIPDB tracks IP addresses that have been associated with malicious activity and makes this information publicly available.

[14] MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) is a knowledge base that details tactics and techniques used in real attacks that is often used as a foundation for the development of an attack.

in this report, which occurred about a month later. The second attempt to compromise was successful in locking out approximately 20 user accounts. There were no functional impacts identified in the report. However, the entity stated the attack strained operational efficiency and the IT service desk handling the account lockouts. Overall, the attackers failed to gain access to any BCS as the controls in place were sufficient.

Report C also did not identify any functional impacts and appears to have been attempting to identify open network ports on the entity's SCADA system. Outside of making the initial connections to the network, there was no intrusion to any BCS and no impacts to BPS reliability. The entity's controls were sufficient to identify and mitigate the attack, as all traffic from the foreign IP was blocked and no further incidents were reported.

Other Key Takeaways: In 2024, the three reports of Cyber Security Incidents are considered attempts to compromise. There were no Reportable Cyber Security Incidents submitted in 2024. The number of reports from 2023 to 2024 remained the same. Two of the three attacks originated from IP addresses in foreign countries, and there was an increased level of sophistication through use of multiple IP addresses in two of the attempted attacks. Unlike the reports of 2022 and 2023, none of the reports mentioned involved third-party or contracted employees. However, based on recent trends, it is still important to remain vigilant of systems operated by both Responsible Entities and those of contracted third parties.

Over the past four years, the E-ISAC has received sixteen 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. There are a total of three CIP-008-6 reports in both 2023 and 2024 and only two reports in 2021. 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 as shown in **Figure 2**. However, there does appear to be a trend of more activity in Q2 and Q3 overall.

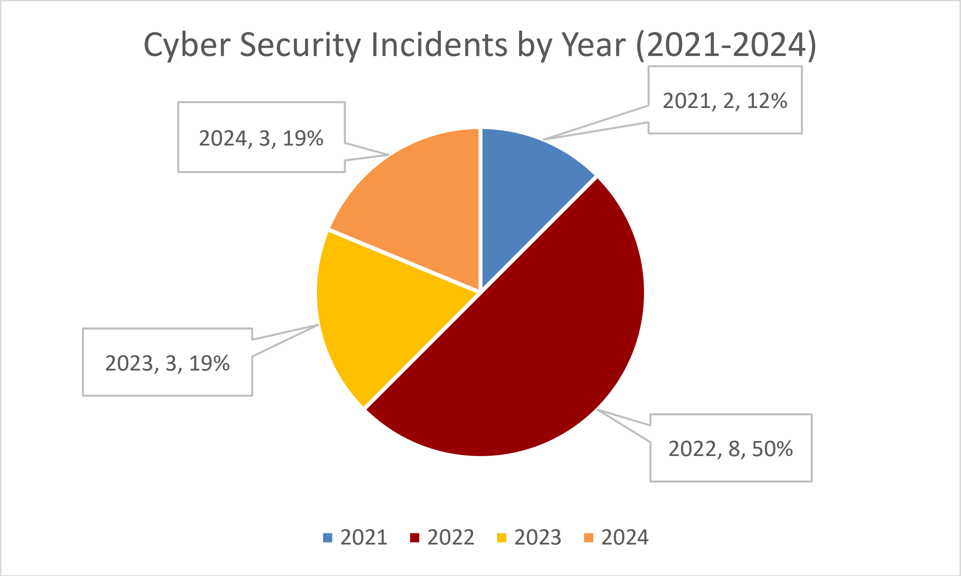

Figure 1. Cyber Security Incidents by Year (2021-2024)

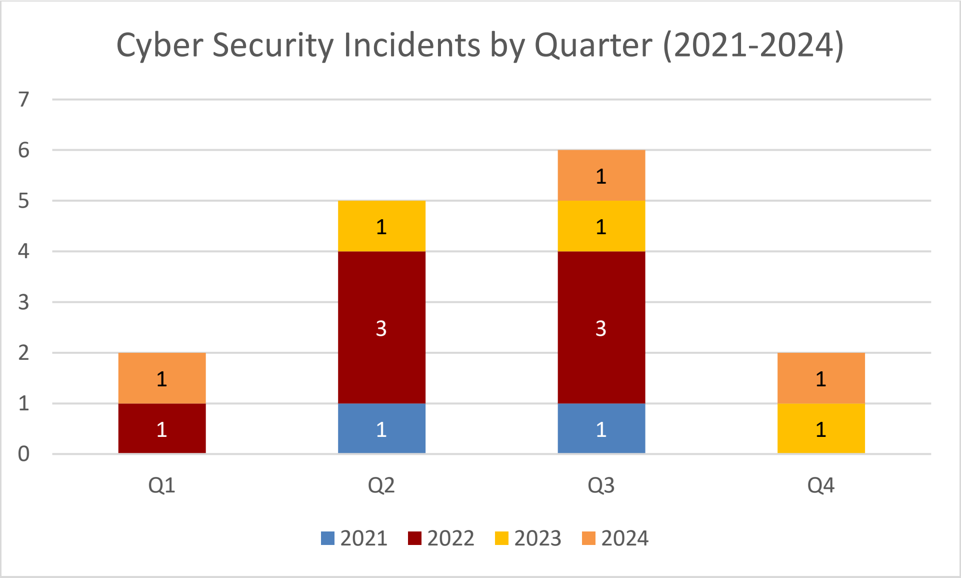

Figure 2. Cyber Security Incidents by Quarter (2021-2024)

Figure 3 shows the breakdown of various attack vectors based on the reports received. The most common attack vector is malware, accounting for approximately 38% of reported incidents, followed by attacks on third parties who support BES operations and brute-force attacks.

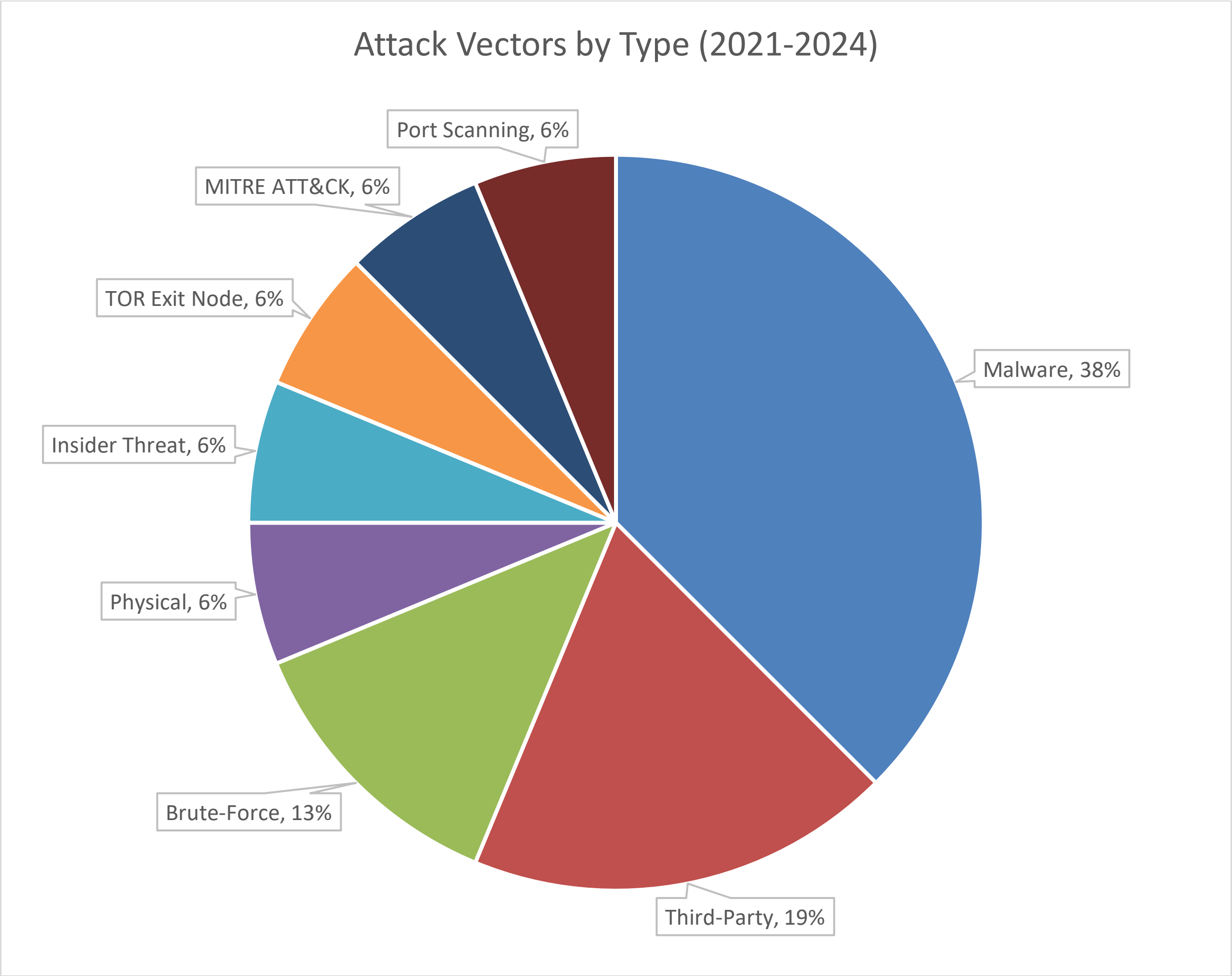

Figure 3. Attack Vectors by Type (2021-2024)

While it appears that malware, such as trojan horses and ransomware, are most common, NERC has not established attack vector trends based on the 16 reports received in the last four years. As part of its annual analysis, NERC continues to look for trends and encourages Responsible Entities to remain vigilant of other attack vectors.

IV. NEXT STEPS

NERC is encouraged that there were no reliability impacts from the reported incidents during the 2024 calendar year and that entities reported these attempts to the E-ISAC. However, each of these Cyber Security Incidents involved attempts on either BCS or systems used to support the reliable operation of the BPS, which highlights the continued need for vigilance.

To enhance the reporting requirements, NERC continues a standards development project, Project 2022-05 – Modifications to CIP-008 Reporting Threshold. This project resulted from the ERO Enterprise review efforts conducted in 2021 and 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, 2025

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, 2025.

/s/ Marisa Hecht

Marisa Hecht
Counsel for North American
Electric Reliability Corporation