Comments of the North American Electric Reliability Corporation

Proposed Rule for the Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements

Cybersecurity and Infrastructure Security Agency Docket ID: CISA-2022-0010

The North American Electric Reliability Corporation ("NERC") respectfully submits comments on the Cybersecurity and Infrastructure Security Agency's ("CISA") Notice of Proposed Rulemaking ("NPRM") for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") reporting requirements.[1] These comments focus on (1) the imperative to harmonize reporting obligations, and (2) the need to develop a mechanism within the CIRCIA reporting rules for the sharing of information with Information Sharing and Analysis Centers ("ISAC").

Critical infrastructure participants continue to face an evolving and relentless threat landscape. Information sharing is an integral component of maintaining cybersecurity and responding to cyber events. Establishing consistent reporting requirements is especially important in facilitating the sharing of security information across critical infrastructure sectors. As recognized by the Office of the National Cyber Director ("ONCD"), "lack of harmonization and reciprocity harms cybersecurity outcomes while increasing compliance costs through additional administrative burdens."[2] As discussed below, NERC appreciates CISA's efforts to implement CIRCIA in a manner that would avoid duplicative reporting requirements and looks forward to working with CISA and the Federal Energy Regulatory Commission ("FERC") to explore options

[1] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 FR 23644 (Apr. 4, 2024) [hereinafter NPRM].

[2] Office of the National Cyber Director, Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information (June 2024), available at https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.

to further minimize unnecessary duplication between NERC's mandatory reporting requirements and CISA's final CIRCIA reporting rule.

NERC, as the operator of the Electricity ISAC ("E-ISAC") on behalf of the electricity sector, also respectfully requests that, in issuing its final CIRCIA reporting rule, CISA consider the role and expertise of ISACs within their respective critical infrastructure sectors. ISACs have a unique ability to use established information sharing mechanisms to enhance situational awareness and amplify CISA's analysis of threats and vulnerabilities within their respective sectors. CISA should leverage ISAC information sharing capabilities by specifying in the final rule that CISA may share CIRCIA reports and CISA's analysis of those reports with ISACs to promote situational awareness and meet the objectives of CIRCIA.

1. Harmonization of Reporting Obligations Improves Cybersecurity Outcomes

As further described in its comments on CISA's Request for Information ("RFI") and recognized in the NPRM,[3] NERC develops mandatory and enforceable reliability standards subject to FERC review and approval pursuant to the authority granted in Section 215 of the Federal Power Act. NERC's Reliability Standards include a family of standards, referred to as the Critical Infrastructure Protection ("CIP") standards, which address cyber and physical security risks. The CIP standards provide a foundation of sound security requirements across the North American bulk power system. NERC Reliability Standards CIP-008-6 (Cyber Security Incident Reporting and Response Planning) and CIP-003-8 (Security Management Controls) include requirements that certain owners, operators, and users of the North American bulk power system report certain cyber security incidents to both CISA and the E-ISAC.[4]

---

[3] See NPRM, Section III.B.

[4] The following types of electricity sector participants are subject to the CIP reporting requirement: Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners.

As CISA also recognized in the NPRM, electric sector participants are also subject to the Department of Energy ("DOE") Form OE-417 reporting requirements. To avoid unnecessary duplication in instances in which both a NERC CIP report and an OE-417 report are required, entities subject to NERC's CIP reporting requirement may submit their OE-417 report in lieu of a separate CIP report.

In its Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information, ONCD recognized that lack of cybersecurity regulatory harmonization and reciprocity poses a challenge to cybersecurity outcomes as regulated entities devote resources on fulfilling the technical requirements of duplicative regulations that could otherwise be devoted to cybersecurity outcomes. NERC thus aims to avoid duplicative and inconsistent reporting requirements that could result in additional regulatory burden on electricity sector participants and impair incident response.

There are many commonalities between CISA's proposed CIRCIA reporting requirement, NERC's CIP reporting requirements, and DOE's Form OE-417. NERC appreciates CISA's statement that it is "committed to working with DOE, FERC, and NERC to explore the applicability of the substantially similar reporting exception to enable, to the extent practicable, entities subject to CIRCIA and CIP Reliability Standards or Form OE-417 reporting requirements to be able to comply with both regulatory reporting regimes through the submission of a single report to the Federal government."[5] NERC looks forward to working with its government partners to explore options to reduce regulatory burden and avoid unnecessary duplication while ensuring robust cyber security reporting requirements.

[5] See NPRM, Section IV.B.iv.2.f.

2. Sharing Reports with ISACs

NERC respectfully requests that CISA include in its final CIRCIA regulations a mechanism for sharing the reports submitted by covered entities and CISA's analysis of those reports with ISACs. As noted above and in NERC's RFI comments, ISACs are uniquely positioned within their critical infrastructure sectors to amplify CISA's analysis throughout their respective sectors and to enrich CISA's analysis with sector-specific information. ISACs are well positioned to play a vital role in accomplishing the objective of CIRCIA of enhancing situational awareness of threats and vulnerabilities and reducing the risk of a cyber incident propagating within and across critical infrastructure sectors.

ISACs were established under a presidential directive in 1998 to enable critical infrastructure owners and operators to share cyber threat information and best practices. Based on the E-ISAC's experience, an ISAC is best able to fulfill that mission when information is readily exchanged between the government and the private sector. Given the E-ISAC's established communication mechanisms and protocols, it is well positioned to receive the CIRCIA reports and CISA's analysis of those reports and cascade CISA's message across the electricity sector. Other ISACs are similarly situated in their sectors as well.

The E-ISAC has an existing arrangement with CISA and the Joint Cyber Defense Collaborative ("JCDC") to share information with the electricity sector proactively before it may become public. Recent collaborations on "Volt Typhoon" and "Cyber Army of Russia Reborn" pre-release information between JCDC and the E-ISAC enabled the electricity subsector to be better positioned for the threat when it became public. This type of proactive operational collaboration and information exchange could further be leveraged with CIRCIA reporting to provide early warning via ISACs on emerging threats.

The E-ISAC understands that in certain instances there may be privacy-related concern with sharing attributable information with ISACs without the consent of the submitting entity. The E-ISAC respectfully requests that CISA develop a process for obtaining consent for sharing attributable information and, where that is not possible, removing identifiable information from the reports and its analysis to be able to share relevant information with ISACs and their members free of any security and privacy-related issues. Sharing of aggregated or anonymized summaries of reports; trending analysis; or analysis of a specific threat, vulnerability, or risk that do not identify any incident at a specific covered entity with the ISACs will still help fulfill the objectives of CIRCIA without implicating any privacy-related issues.

3. Conclusion

NERC appreciates the opportunity to comment on the proposed rule and looks forward to continued coordination.

Respectfully submitted,

Shamai Elstein
Shamai Elstein
Associate General Counsel
North American Electric Reliability Corporation
1401 H St., NW
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net

Counsel for North American Electric Reliability Corporation