Request for Information on the
Cyber Incident Reporting for Critical Infrastructure Act of 2022

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

Joint Comments of the North American Electric Reliability Corporation
and the Regional Entities

The North American Electric Reliability Corporation ("NERC") and the six Regional Entities,[1] collectively the "Electric Reliability Organization ("ERO") Enterprise," submit comments on the Cybersecurity and Infrastructure Security Agency ("CISA") Request for Information ("RFI") on proposed regulations required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). The ERO Enterprise's comments reflect lessons learned from its development and enforcement of mandatory cybersecurity incident reporting requirements applicable to certain electricity sector asset owners and operators. The comments also reflect NERC's operation of the Electricity Information Sharing and Analysis Center ("E-ISAC").

Electricity sector and other 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. Through the reporting requirements to be issued under CIRCIA, CISA has a significant opportunity to act as a valuable partner in tracking and responding to cyber threats to critical infrastructure.

Establishing consistent reporting requirements is especially important in facilitating the sharing of security information across critical infrastructure sectors. These comments emphasize that there may be substantial overlap and inconsistencies between the ERO Enterprise reporting

[1] The six Regional Entities include the following: Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council.

requirements and those to be issued under CIRCIA. To avoid duplicative and inconsistent reporting requirements that could result in additional regulatory burden on electricity sector participants and impair incident response, the ERO Enterprise respectfully requests continued coordination with CISA to ensure harmonization between the ERO Enterprise and CIRCIA incident reporting requirements.

The ERO Enterprise also respectfully requests that in issuing its regulations, CISA consider the role of ISACs within their respective critical infrastructure sectors, including their ability to use established communications mechanisms and already in place information sharing, such as the Cybersecurity Risk Information Sharing Program ("CRISP"), to enhance situational awareness and amplify CISA's analysis of threats and vulnerabilities.

I. Description of ERO Enterprise

NERC is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the North American bulk power system. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico.

In the United States, the Federal Energy Regulatory Commission ("FERC") certified NERC as the designated ERO under Section 215 of the Federal Power Act. As the ERO, NERC is charged with developing and enforcing mandatory Reliability Standards applicable to owners, operators and users of the bulk power system; assessing current and future reliability trends; analyzing system events; and recommending improved practices. NERC accomplishes its mission with the support of the six Regional Entities. The six Regional Entities support reliability across differing interconnections with specific needs and characteristics by conducting compliance monitoring, enforcement, analysis, and outreach activities, among other things.

NERC's mandatory and enforceable Reliability Standards, which are approved by FERC in the U.S., define the reliability requirements for planning and operating the North American bulk power system. 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. As discussed further below, NERC Reliability Standards CIP-008-6 (Cyber Security Incident Reporting and Response Planning) and CIP-003-8 (Security Management Controls) include incident reporting for certain cyber systems associated with bulk power system operations that are similar to those required under CIRCIA. Additionally, Reliability Standard EOP-004-4 (Event Reporting) requires reporting of certain events, such as damage to facilities and loss of capabilities, among others.[2]

In addition to its role of developing and enforcing mandatory Reliability Standards, NERC also operates the E-ISAC on behalf of the electricity industry. The E-ISAC provides its members and partners with resources to enhance situational awareness and prepare for and reduce cyber and physical security threats to the North American electricity industry.

II. Comments

a. Coordination and Consistency with NERC Reliability Standards

As noted above, NERC Reliability Standards CIP-008-6 and CIP-003-8 include cyber incident reporting requirements applicable to the following types of electricity sector participants included on NERC's Compliance Registry: Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and

[2] NERC Reliability Standards are available at: https://www.nerc.com/pa/Stand/Pages/default.aspx.

Transmission Owners.[3] As described below, the incident reporting requirements in CIP-008-6 and CIP-003-8 are similar to the reporting requirements set out in CIRCIA, although there are some differences. To avoid duplicative and inconsistent reporting requirements that could impair the sharing of security information across critical infrastructure sectors and that could cause additional regulatory burden on electricity sector participants subject to NERC Reliability Standards, the ERO Enterprise respectfully requests continued coordination with CISA to ensure harmonization between the ERO Enterprise and CISA's CIRCIA reporting requirements.[4]

The following is a description of NERC's existing incident reporting requirements applicable to the operational technology environment of electric sector participants.

Reliability Standard CIP-008-6 requires Responsible Entities[5] to develop and implement cyber security incident response plans. These incident response plans must provide a course of action for Responsible Entities to detect and respond to incidents that affect cyber systems located in or associated with higher risk transmission and generation assets and control centers.[6] The requirements in Reliability Standard CIP-008-6 specify processes and procedures to be included in Cyber Security Incident response plans, implementation and testing of these plans, and maintenance of these plans. Among other things, the standard also requires entities to report certain cyber security incidents affecting their applicable cyber systems to both the E-ISAC and CISA as

---

[3] These terms are defined in NERC's Glossary of Terms Used in NERC's Reliability Standards, available here: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[4] As an example of this coordination, the Department of Energy coordinated with the ERO Enterprise to align its Form DOE-417 with NERC's reporting requirements in CIP-008-6. NERC accepts submission of DOE-417 for compliance with CIP-008-6. *See* https://www.federalregister.gov/documents/2020/06/12/2020-12689/agency-information-collection-extension.

[5] As used in the Critical Infrastructure Protection ("CIP") Reliability Standards, a Responsible Entity refers to the registered entities subject to the CIP Reliability Standards.

[6] NERC's incident reporting requirements do not apply to all cyber systems used by NERC registered entities, only those associated with bulk power system operations (i.e., operational technology systems not information technology systems). For example, a corporate accounting system that is isolated from an entity's operational technology systems would not be subject to the CIP standards. CIRCIA reporting requirements applicable to those corporate systems would not overlap with NERC's reporting requirements.

part of their incident response to facilitate information sharing on cyber threats and vulnerabilities across the sector.

The incident reporting requirement in CIP-008-6 contains the following components:

- Types of Incidents to be Reported: CIP-008-6 requires entities to report (1) "Reportable Cyber Security Incidents", generally defined as a cyber security incident that has operational impact or successfully compromises an Electronic Security Perimeter ("ESP")[7] or Electronic Access Control or Monitoring System ("EACMS");[8] and (2) Cyber Security Incidents that are "attempts to compromise" a Bulk Electric System ("BES") Cyber System or associated EACMS. CIP-008-6 requires each entity to develop a process to define what constitutes an "attempt to compromise" a BES Cyber System, ESP or EACMS.
- Timeline for Reporting: Initial reports for Reportable Cyber Security Incidents must be submitted within one hour of determination. Attempts to compromise a BES Cyber System, ESP or EACMS must be submitted by the end of the next calendar day following determining there was an attempt. Entities are also required to submit updated reports within seven days if there is any new or changed information.
- Contents of Report: Reports must include the following, if known at the time of reporting: (1) the functional impact of the incident; (2) the attack vector used; and (3) the level of intrusion achieved or attempted.

CIP-003-8 applies to cyber systems associated with lower risk transmission and generation assets and control centers. Among other things, CIP-003-8 requires entities to develop incident response plans for these lower risk assets that include notification to the E-ISAC of Reportable

[7] An ESP is defined as the logical border surrounding a network to which BES Cyber Systems are connected. A BES Cyber System are generally those cyber assets used for bulk power system operations.

[8] An EACMS is defined as cyber assets that perform electronic access control or monitoring of an ESP or BES Cyber Systems.

Cyber Security Incidents. Given the lower level of risk, entities are not currently required to report on attempts to compromise under CIP-003-8.

EOP-004-4 requires certain entities to have an event reporting Operating Plan that includes protocols for reporting events to the ERO and other relevant organizations.[9] Certain events identified in EOP-004-4 must be reported the later of 24 hours of recognition of meeting an event type threshold or by the end of the entity's next business day (4 p.m. local time). Those entities may also submit a DOE-417 form to the ERO in lieu of the form provided in EOP-004-4.

The incident reporting requirements that CISA is developing under CIRCIA could potentially overlap with the requirements in NERC Reliability Standards CIP-008-6 and CIP-003-8. Given the likely overlap, CISA should consider whether to classify the NERC reports as "substantially similar" under CIRCIA.

Additionally, in certain instances, there may be some inconsistent requirements between NERC and CISA reporting. For instance, entities subject to both NERC reporting requirements and CISA reporting regulations would potentially have different timelines for reporting and the reports may require different information. The ERO Enterprise seeks to avoid duplicative and inconsistent reporting requirements that would cause additional regulatory burden on electricity sector participants that could hinder incident response. The ERO Enterprise respectfully requests continued coordination with CISA to ensure harmonization between the ERO Enterprise and CISA's CIRCIA reporting requirements.

[9] Depending on the entity's functional registration, an entity must report the following according to Attachment 1 to the standard: (1) Damage or destruction of a Facility; (2) Physical threat to its Facility; (3) Physical threat to its BES control center; (4) BES Emergency (firm load shedding, public appeal for load reduction, System-wide voltage reduction, voltage deviation on a Facility, uncontrolled loss of firm load); (5) System separation (islanding); (6) Generation loss; (7) Complete loss of off-site power to a nuclear generating plant (grid supply); (8) Transmission loss; (9) Unplanned evacuation of its BES control center; (10) Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability at its staffed BES control center; (11) Complete loss of monitoring or control capability at its staffed BES control center.

b. "Covered Cyber Incident" and "Substantial Cyber Incidents"

Based on the ERO Enterprise's experience developing and enforcing mandatory cyber incident reporting requirements, the value of CIRCIA's reporting will, in large part, depend on the manner in which CISA defines "Covered Cyber Incident" and "Substantial Cyber Incidents." If defined too broadly (e.g., requiring reports of phishing attempts), it could be overly burdensome on industry and CISA would likely be inundated with reports. It would require CISA to expend significant effort to separate the noise from actionable information. If defined too narrowly, many incidents may go unreported and CISA will have an incomplete picture of the threat landscape. If defined to provide covered entities too much discretion to determine whether an incident is reportable, the reporting will likely be inconsistent across covered entities and leave CISA with an incomplete picture of the threat landscape.

In developing its incident reporting requirements, the ERO Enterprise initially required entities to report only incidents that had operational impact (i.e., Reportable Cyber Security Incidents). Over the years, however, there were very few incidents reported. While receiving few reportable incidents is a positive insofar as it means that there were very few cyber incidents that had an impact on electric utility operations, it could also miss reporting on significant cyber activity, leaving industry unaware of emerging threats and vulnerabilities that have yet to have operational impact. To address that issue, FERC directed NERC to require entities to report attempts to compromise a BES Cyber System, ESP, or EACMS to the E-ISAC and CISA. The objective was to have a broader insight into the threat landscape and provide increased awareness of threats facing the electricity industry.

In an attempt to balance the need for additional reporting and burden on industry, the NERC Reliability Standard does not precisely define an attempt to compromise. Instead, Responsible

Entities must implement a process that includes criteria to evaluate and define attempts to compromise. As a result, there is a significant degree of flexibility permitted in what types of incidents entities may report when it comes to attempts to compromise. The rationale behind this language was that what was considered "suspicious" or an "attempt" would vary across operating environments, and Responsible Entities needed to determine that for their own circumstances.

As Responsible Entities began implementing the provisions in Reliability Standard CIP-008-6 regarding attempts to compromise, which began in January 2021, there were few additional reports submitted. Between the dates of January 1, 2021 and December 31, 2021, Responsible Entities submitted two CIP-008-6 reports to the E-ISAC. These two reports include attempts to compromise applicable systems but did not have operational impact. The ERO Enterprise initiated a study to gain a better understanding of how registered entities fulfill their obligations to categorize cyber security incidents, including attempts to compromise. The ERO Enterprise engaged with 25 entities to complete the study. The study concluded the current language of the Reliability Standard permits the use of subjective criteria to define attempts to compromise, and most programs include a provision allowing a level of staff discretion.

Based on the study, the ERO Enterprise is initiating a standards development project to revise the reporting requirements in CIP-008-6. The objective of the project is to revise Reliability Standard CIP-008-6 to provide a minimum expectation for thresholds defining attempts to compromise. These thresholds should not be so prescriptive as to require the reporting of every internet facing firewall port scan, phishing email identified, or file alerted by endpoint anti-virus scans. Rather, the intent would be to right size the reporting threshold to improve visibility of existing and future cyber security risks to the BES. In the fourth quarter of 2022 NERC will form a standard drafting team of industry subject matter experts, who will begin working on revisions

in 2023. The ERO Enterprise anticipates filing the revised standard for FERC approval by the end of 2023.

In addition to considering this lesson learned for CIP-008-6 regarding setting minimum expectations for reporting, particularly when it comes to cyber security incidents that do not have operational impact, the ERO Enterprise has significant experience collecting and sharing information through the E-ISAC. Based on its experience, the E-ISAC recommends that the definition of "covered cyber incident" cover the following:

- Unexpected or anomalous external routable connectivity not through established electronic access points.
- Unexpected or anomalous multi-factor authentication attempts or sessions.
- Unexpected or anomalous remote access by vendor into entities network(s) (IT/OT).
- Unexpected or anomalous activity from logical network accessible ports.
- Presence of malicious code in an organization's environments (malicious code determined a Key Vulnerability by CISA).
- Detected failed access attempts and failed login attempts from malicious code or known vulnerabilities identified by CISA.
- Unexpected, anomalous, or unauthorized activity by privileged access management accounts.
- High number of unsuccessful authentication attempts as determined by organization baseline in IT and OT systems.
- Any incident that disrupts operations of critical infrastructure (e.g., disruption of generation, transmission, and/or distribution assets in electricity).
- An attempt to compromise operations of critical infrastructure (e.g., a deliberate or inadvertent attempt to disrupt generation, transmission, and/or distribution assets in electricity).
- A deliberate or inadvertent attempt to slow down or disrupt routable network operations for more than five minutes in a determined critical infrastructure network (IT and/or OT).

- Unexpected or anomalous change to the baseline activity of the IT or OT network, including unauthorized applications, remote access to system outside of baseline activity hours, or geographically impossible logins or login attempts.

- Exploitation of Key Vulnerabilities as identified by CISA in an organization's environment.

- Unexpected, anomalous, or unauthorized access of critical systems of operational critical infrastructure assets for on-premise data storage, security during transit.

- Unexpected, anomalous, or unauthorized access of off-premise or cloud data storage critical systems of operational critical infrastructure assets, including: encryption, hashing, tokenization, cipher, electronic key management failures.

- Inappropriately disposed of critical electronic assets.

- Appearance on cybercriminal forums (as determined by FBI) or nefarious assets of sensitive critical infrastructure data.

- Unexpected, anomalous, or unauthorized modification of real-time monitoring data or assessment between control centers operating critical infrastructure.

- Disclosure by a vendor or supply chain entity in an organization's supply chain (even if no impact on the organization) to assess extent of condition and overall risk.

c. Report Submission Procedures

Based on its lessons learned from administering the reporting requirement in CIP-008-6, the ERO Enterprise recommends that CISA (1) require covered entities to clearly identify that an incident is being reported pursuant to CIRCIA, as opposed to a voluntary share, and (2) develop an automated mechanism to confirm receipt of a CIRCIA report from a covered entity or a third party on behalf of a covered entity.

Requiring entities to clearly identify that a report is being submitted pursuant to CIRCIA requirements will create efficiencies for CISA as it processes that information and considers enforcement of those requirements.

Given potential enforcement of its regulations, it is also important that CISA develop a mechanism for confirming receipt of submission for covered entities. This is especially true if a

covered entity chooses to submit through a third party, like the E-ISAC. Given the existing requirement to report incidents to the E-ISAC through CIP-008-6, many entities in the electricity sector may seek to rely on the E-ISAC to submit the report to CISA (through an automated mechanism on the E-ISAC portal or otherwise). Under CIRCIA, however, the duty to report remains on the covered entity. Proving a confirmation of receipt would create efficiencies for the third party and covered entity to demonstrate that the report was submitted on time.

d. Sharing of Submissions with ISACs

NERC respectfully requests that CISA include in its regulations implementing CIRCIA a mechanism for sharing the reports submitted by covered entities and CISA's analysis of those reports with ISACs. ISACs are uniquely positioned within their critical infrastructure sectors to amplify CISA's analysis throughout their respective sectors. ISACs can play a large role in accomplishing the objective of CIRCIA to enhance situational awareness of threats and vulnerabilities and reduce the risk of a cyber incident propagating within and across 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 understands that in certain instances there may be privacy-related concerns with sharing attributable information with ISACs without the consent of the submitting entity. The E-ISAC respectfully requests that, when necessary, 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 so as 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.

III. Conclusion

The ERO Enterprise appreciates the opportunity to comment on the RFI and looks forward to continued coordination.

Respectfully submitted,

/s/ Shamai Elstein

Shamai Elstein
Associate General Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, DC 20005
(202) 400-3000
shamai.elstein@nerc.net
marisa.hecht@nerc.net
Counsel for the North American Electric Reliability Corporation

/s/ Niki Schaefer
Niki Schaefer
Vice President & General Counsel
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, Ohio 44131
(216) 503-0600
(216) 503-9207 - facsimile
niki.schaefer@rfirst.org
Counsel for ReliabilityFirst Corporation

/s/ Holly A. Hawkins
Holly A. Hawkins
Vice President, General Counsel, and Corporate Secretary
SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273
(704) 357-7372
hhawkins@serc1.org
Counsel for the SERC Reliability Corporation

/s/ Derrick Davis
Derrick Davis
General Counsel & Corporate Secretary
Texas Reliability Entity, Inc.

/s/ Lisa A. Zell
Lisa A. Zell
Vice President General Counsel and Corporate Secretary
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(651) 855-1760
lisa.zell@mro.net
Counsel for Midwest Reliability Organization

805 Las Cimas Parkway, Suite 200
Austin, TX 78746
(512) 583-4900
derrick.davis@texasre.org
Counsel for Texas Reliability Entity, Inc.

/s/ Jeff Droubay
Jeff Droubay
Vice President and General Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6879
jdroubay@wecc.org
Counsel for the Western Electricity Coordinating Council

/s/ Damase Hebert
Damase Hebert
Associate General Counsel & Director, Enforcement
Northeast Power Coordinating Council, Inc.
1040 Ave. of the Americas, 10th Floor
New York, NY 10018
(212) 840-1070
dhebert@npcc.org
Counsel for Northeast Power Coordinating Council, Inc.

Date: November 14, 2022