Cybersecurity and Infrastructure Security Agency
Washington, D.C. 20585

Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022	)))))	**Docket CISA-2022-0010**

COMMENTS OF THE ELECTRIC POWER SUPPLY ASSOCIATION ON THE REQUEST FOR INFORMATION

Pursuant to its September 12, 2022 publication in the Federal Register,[1] the Electric Power Supply Association ("EPSA")[2] submits the following response to the U.S. Cybersecurity and Infrastructure Security Agency's ("CISA") Request for Information ("RFI") on its approach to implementing cyber incident and ransom payment reporting requirements as directed by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").[3] EPSA appreciates the opportunity to provide feedback to CISA on issues of such importance.

EPSA members – which include competitive power suppliers and independent power producers – operate under a myriad of cyber and physical security regulatory regimes. Notably, EPSA members participate in the development of, and comply with, North American Electric Reliability Corporation ("NERC") Critical Infrastructure

---

1 87 FR 55833, pp 55833-55836, Document number 2022-19551, (published September 12, 2022).

2 EPSA is the national trade association representing competitive power suppliers in the U.S. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. EPSA seeks to bring the benefits of competition to all power customers. This pleading represents the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.

3 *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Public Law No. 117-105, (March 15, 2022).

Protection ("CIP") standards,[4] which work to ensure the appropriate security measures are in place to protect the entirety of the Bulk Electric System ("BES").

Partnerships between EPSA members and government agencies responsible for cybersecurity exist at every stage of operations. EPSA is a member of the Electricity Subsector Coordinating Council Secretariat ("ESCC"); the ESCC serves as the principal liaison between leadership across multiple federal agencies and the electric power sector. Companies also participate in bi-directional information sharing with U.S. intelligence as well as industry and government partners. As CISA's rule could include duplicative concepts, EPSA asks that CISA consider existing standards and regulations where applicable in order to maximize efficiency and allow for deference to more stringent existing regimes.

I. COMMENTS

A. NERC Standards Offer a Useful Roadmap for CISA Reporting Requirements

As the objective of NERC standards is to preserve BPS reliability, they are stringent in nature and undergo extensive development and vetting with electric industry experts before final approval by both NERC and the Federal Energy Regulatory Commission ("FERC"). Thus, many of the terms and concepts that the RFI seeks to define have long been in place for the electric power sector. For example, the RFI seeks to define the term "covered cyber incident." Among other relevant definitions, the NERC Glossary of Terms already includes a definition for a "Reportable Cyber Security Incident." NERC defines a "Reportable Cyber Security Incident" as a Cyber Security

[4] *See generally,* North American Electric Reliability Corporation, Critical Infrastructure Protection Standards, https://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx.

Incident that compromised or disrupted: (1) a BES Cyber System that performs one or more reliability tasks of a functional entity; (2) an Electronic Security Perimeter of a high or medium impact BES Cyber System; or (3) an Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.[5] As it pertains to the electric power sector, EPSA suggests that this would be an appropriate definition with which CISA should align. Should CISA seek to craft a more generic definition to span multiple sectors, these criteria represent an extensively vetted guidepost that CISA could follow.

The RFI also asks what constitutes "reasonable belief" that a covered cyber incident has occurred. Here again, NERC provides a helpful example. Under the term "Reportable Cyber Security Incident," the "reasonable belief" standard is absent in recognition of the fact that these events can have different impacts on different entities. Accordingly, under NERC CIP standards, each entity maintains an incident reporting and response plan that lays out how it would respond to certain cyber events.

NERC CIP recognizes that the determination of what constitutes an elevated cyber event is unique to each company and industry. These determinations are typically based on multiple factors, including the nature of the incident, type of assets affected, the classification of systems affected, and type of environment breached (Corporate or Operational Technology). Essentially, even within the electric power sector there is recognition that utilizing a "one size fits all" approach presents practical challenges which diminishes the usefulness of that approach. As the instant NOPR process will ultimately include a multitude of other industries, an overly prescriptive approach may

[5] North American Electric Reliability Corporation, Glossary of Terms Used in NERC Reliability Standards, (Updated March 29, 2022), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

prove unwieldy. Accordingly, EPSA suggests that CISA should allow for flexibility in its definitions, recognizing that entities – particularly those that own and operate critical infrastructure – know their operations and, in the case of electric power providers, have existing reporting and response plans already in place which can be used to respond to CISA as well.

B. Reporting Requirements

CIRCIA posits that a cyber incident should be reported within 72 hours. Here again, NERC CIP has an existing and more stringent standard in place. For instance, under CIP-008-6, R4 mandates that high and medium impact entities must notify NERC's Electricity Information Sharing and Analysis Center and the United States National Cybersecurity and Communications Integration Center within "one hour after the determination of a Reportable Cyber Security Incident" or "by the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the 'Applicable Systems' column…"[6] This standard also prescribes the criteria that must be included in each notification.[7] In addition, while not in CIP standards, given their role in maintaining critical infrastructure, electric power entities typically notify the FBI out of an abundance of caution depending on the nature of the incident. Given that the electric industry is already reporting these incidents via multiple channels, it might be more efficient for CISA to establish a line of communication with

---

[6] North American Electric Reliability Corporation, Cyber Security — Incident Reporting and Response Planning, Standard CIP-008-6, R4, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-008-6&title=Cyber%20Security%20%E2%80%94%20Incident%20Reporting%20and%20Response%20Planning&Jurisdiction=United%20States.

[7] *Id.*

these entities to create a process that automatically sends these reports to CISA, rather than adding another step to an already existing process.

II. CONCLUSION

EPSA appreciates the opportunity to comment on these important issues and respectfully requests the CISA allow for flexibility and deference in crafting its NOPR, recognizing that some industries are already subject to more stringent requirements than may be required in the CISA NOPR. Hence, CISA should use these exiting standards (such as NERC CIP) as a roadmap in defining terms in its proposed rule in order to maintain clarity, consistency, and efficiency in reporting and recordkeeping. Such action will result in a more streamlined and useful rollout of the requirements in a CIRCIA final rule.

Respectfully submitted,

ELECTRIC POWER SUPPLY ASSOCIATION

By: *Bill Zuretti*
Bill Zuretti
Director, Regulatory Affairs & Counsel
Electric Power Supply Association
1401 New York Ave, NW, Suite 950
Washington, DC 20005

Dated: November 14, 2022