CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
WASHINGTON, D.C. 20585

Cyber Incident Reporting for Critical Infrastructure Reporting Requirements	))))	Docket CISA-2022-0010

COMMENTS OF THE ELECTRIC POWER SUPPLY ASSOCIATION

Pursuant to the April 4, 2024 publication in the Federal Register,[1] the Electric Power Supply Association ("EPSA")[2] submits the following response to the Cybersecurity and Infrastructure Security Agency's ("CISA") Notice of Proposed Rulemaking ("NPRM") to implement the reporting requirements of 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 – 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 Protection ("CIP") standards, which work to ensure the appropriate security measures are in place to protect the entirety of the Bulk Electric System. In addition, partnerships between EPSA members and government agencies responsible for cyber security exist at every stage

[1] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644, 23,766 (published Apr. 4, 2024). ("NPRM")

[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).

of operations. EPSA also works closely with the Electricity Subsector Coordinating Council ("ESCC") which 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 entities as well as industry and government partners.

CISA's proposed rule is extremely broad and therefore could involve more extensive reporting than the detailed regimes under which EPSA members currently operate and which are useful in addressing and mitigating national security concerns. In light of the coverage and information provided by these existing structures, EPSA recommends that CISA refine its proposed requirements establishing what constitutes a covered cyber incident in a manner that avoids requiring covered entities to utilize valuable time and resources reporting on less critical incidents simply to comply with CISA's rule rather than to strengthen facilities' cybersecurity protections. In addition, given that the electric industry is already reporting these incidents via multiple channels, EPSA requests CISA to establish a line of communication with these entities to create a process that automatically sends these reports to CISA, rather than adding another step by establishing a new but duplicative process.

I. COMMENTS

A. CISA Should Narrow Its Reporting Criteria and Harmonize the Reporting Process

Among other requirements, CIRCIA directs CISA to promulgate regulations requiring critical infrastructure entities ("covered entities") to report covered cyber incidents and Ransom payments to CISA within 72 and 24 hours, respectively. Currently, EPSA members are already required to report high and medium asset cyber

incidents under NERC CIP, which has an existing and more rigorous standard in place for those incidents. CISA should make a similar more specific reporting criteria which excludes countless low-impact asset incidents. For instance, under CIP-008-6, R4 mandates that for high and medium-impact BES assets, entities must notify NERC's Electricity Information Sharing and Analysis Center ("E-ISAC") 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…"[4]

To date, this regime has been effective because it provides a clearly defined standard which requires companies to expeditiously report incidents from those facilities – high and medium-impact BES assets – that are of consequential importance to the grid in order to ensure the system is not adversely impacted at a level which threatens system operations or reliability. This existing reporting program carries a manageable and meaningful compliance burden on the electric sector. The consideration of even a 72-hour reporting mandate on low-impact BES assets would create a very extensive burden with little or no concomitant benefit. As a result, the instant NPRM, if implemented, would place a much broader burden on the electric industry that would require considerable time and resources and may not yield better results.

[4] 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.

In the NPRM, CISA provides examples of incidents that are "likely to be considered" substantial cyber incidents but then goes on to state that the actual determination of whether a cyber incident is a Substantial cyber incident will be made on a case-by-case basis specific to the circumstances.[5] To overcome this vague and subjective criteria, CISA encourages reporting *all* cyber incidents. Such an overly broad reporting regime could divert critical resources and deploy them merely to *report* incidents rather than to *respond* to them and secure compromised systems. To prevent this undesirable result, CISA should narrow the criteria pertaining to what incidents need to be reported in a manner consistent with spirit of the CIRICA law – namely major cyber security incidents. In reasonably limiting the scope of what needs to be reported, compromised entities can focus on recovering and, likewise, CISA can focus on helping entities recover and limiting damage throughout the broader cyber ecosystem to the greatest extent possible.

For the electric sector, narrowing what is included as a covered cyber incident would yield even greater efficiency – and effectiveness – in reporting because the sector already reports cyber incidents via multiple channels. Should CISA align the NPRM's definitions to more closely mirror existing reporting requirements, CISA will be able to exercise the "substantially similar" exemption that CIRCIA contemplates. This exemption can be triggered when the information required by the fields in CISA's CIRCIA Report forms is functionally equivalent to the information required to be reported by the covered entity to another federal agency.[6] Accordingly, EPSA asks that CISA attempt to

---

5 NPRM, 89 Fed. Reg at 23,668.

6 *Id.* 89 Fed. Reg at 23647.

streamline its rulemaking to complement existing regulations to more effectively implement the mission of CIRCIA and limit duplicative reporting requirements.

In addition, to further streamline and expand the sharing of this information, EPSA requests that CISA establish a line of communication with other entities that currently receive cyber incident reports to create a process that automatically sends these reports to CISA, rather than adding another step to multiple already existing processes. The Biden Administration has recognized the value of harmonizing existing reporting regimes[7] and thus CISA should extend this concept to the instant NPRM. If the reporting criteria or definitions are not narrowed or harmonized, the 72-hour breach reporting requirement would be an unreasonable burden on the electric sector.

B. Data Confidentiality Must be Ensured

As currently proposed, the NPRM requires that all submissions by covered entities be marked in order to receive confidential treatment and be exempt from Freedom of Information Act requests. Reports submitted under this rule are likely to contain highly sensitive information that, if released, could present threats to the security of the grid, and, ultimately, national security. As such, EPSA requests that *all* submissions be given blanket confidentiality, without the added step of marking these reports as such. The sensitivity of this data further buttresses the need to narrow the breadth of what should be reported, as overreporting could unnecessarily expose sensitive information through the process of reporting minor events. Thus, EPSA requests that CISA treat all submissions as confidential, exempt from FOIA, and establish mechanisms to ensure that these sensitive submissions are protected.

---

[7] The White House, *National Cybersecurity Strategy,* (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

II. CONCLUSION

EPSA appreciates the opportunity to comment on these important issues and respectfully requests that CISA refine its proposed requirements for what constitutes a covered cyber incident in a manner that avoids the expenditure of unnecessary time and resources reporting on less critical incidents. In addition, given that the electric industry is already reporting these incidents via multiple channels, EPSA recommends that CISA create a process that automatically shares these reports with CISA, rather than adding an additional new but duplicative reporting burden. Finally, it is important that reports submitted to or shared with CISA are treated as confidential.

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: July 3, 2024