COMMENTS OF THE
AMERICAN PUBLIC POWER ASSOCIATION ON
THE DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE
SECURITY AGENCY NOTICE OF PROPOSED
RULEMAKING ON CYBER INCIDENT REPORTING
FOR CRITICAL INFRASTRUCTURE ACT
REPORTING REQUIREMENTS

Docket Number: CISA-2022-0010

July 3, 2024

The American Public Power Association (APPA) appreciates the opportunity to submit these comments on the Cybersecurity and Infrastructure Security Agency (CISA) Notice of Proposed Rulemaking (NPRM) to implement the requirements of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

APPA is the national trade organization representing the interests of the nation's 2,000 not-for-profit, community-owned electric utilities. Public power utilities are in every state except Hawaii. They collectively serve over 54 million people in 49 states and five U.S. territories, and account for 15 percent of all sales of electric energy (kilowatt-hours) to end-use customers. Public power utilities are load-serving entities, with the primary goal of providing the communities they serve with safe, reliable electric service at the lowest reasonable cost, consistent with good environmental stewardship. This orientation aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities.

Public power utilities know that a reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. Public power utilities take very seriously their responsibility to maintain a secure and reliable electric grid. APPA works closely with its members and federal government partners to improve the security posture of public power utilities with respect to a range of cyber threats.

Introduction and Summary

The NPRM is an important step in implementing CIRCIA and facilitating the federal government's ability to rapidly deploy resources and render assistance to victims of cyber attacks. APPA supports many aspects of the NPRM: it properly requires reporting of actual—not attempted—attacks and of ransom payments—not ransom requests; it properly preempts state and local freedom of information laws; and it avoids draconian enforcement mechanisms.

APPA also believes that the electric industry would benefit from several clarifications to the proposed rule. In these comments, APPA requests clarification on the factors in determining whether a cyber incident is reportable, the timeline for making that determination, and CISA's expectations for the level of detailed information that must be reported in the initial hours following an incident.

Despite the NPRM's many positive elements, APPA strongly urges CISA to make two essential changes before finalizing the rule.

First, CISA should exclude small, distribution-only electric utilities from the reporting obligation. The NPRM proposes to require *all* electric utilities to report significant cyber incidents to CISA. While such an obligation is appropriate for large utilities that serve millions of customers, it is unnecessary and burdensome to impose the same obligation on the hundreds of community-owned, not-for-profit electric utilities that qualify as small businesses. At minimum, such small utilities should be required to report to CISA only if they experience an actual electrical outage that results from a cyber incident.

Second, CISA must complete its intended harmonization efforts with other federal reporting requirements for the electric industry *before* finalizing the rule. The electric sector is already subject to mandatory federal reporting requirements to the Department of Energy (DOE) and North American Electric Reliability Corporation (NERC). If CISA proceeds to finalize its rule prior to reaching agreement with DOE and NERC to share information, many electric utilities will be subject to duplicative reporting requirements contrary to congressional intent.

The NPRM invites public comment on all aspects of the proposed regulations, but notes that CISA is particularly interested in comments on nine specific issues.[1] Table 1, below, summarizes APPA's position on each of those issues and identifies the section(s) of these comments that fully discuss APPA's position on those issues.[2]

[1] NPRM, § I.

[2] The NPRM also seeks comments on data preservation requirements and procedures for protecting privacy and civil liberties. APPA is not taking a position on those issues.

Table 1

NPRM Comment Request	Summary of APPA Position	Reference
Proposed Definitions	APPA supports excluding unsuccessful intrusion attempts from the "covered cyber incident" definition.	Section H
Applicability	APPA strongly urges CISA to modify the scope of entities to exclude small businesses.	Section A
Examples of Reportable Covered Cyber Incidents	APPA seeks clarification on relevant factors in determining an incident's seriousness and on the definition of "business or industrial operations."	Sections D & E
Reporting Requirements and Procedures	APPA urges CISA to harmonize its reporting requirements with electricity regulators and facilitate a single reporting mechanism.	Sections B & C
Report Submission Deadlines	APPA seeks clarification on the amount of preliminary analysis needed to form a reasonable belief that a covered cyber incident has occurred and on how much information is required in the initial report.	Sections F & G
Enforcement Procedures	APPA supports the enforcement procedures, particularly the limitations on penalties for false statements.	Section I
Treatment of Information and Restrictions on Use	APPA supports the preemption of state and local freedom of information laws.	Section J

Comments

A. CISA should exclude electric utilities that are small businesses from the definition of covered entities.

Without explicitly saying so, the NPRM makes all electric utilities, regardless of size, covered entities. Proposed § 226.2(b)(6) establishes the sector-based criteria for electric utilities as any entity "required to report cybersecurity incidents under the North American Electric Reliability Corporation Critical Infrastructure Protection Reliability Standards or required to file an Electric Emergency Incident and Disturbance Report DOE-417 form, or any successor form, to the Department of Energy."

The NPRM's "covered entities" definition is unreasonable for three reasons. First, it dramatically increases the reporting obligation for small electric utilities. DOE Form DOE-417[3] broadly applies to all electric utilities, but only requires them to report on a narrow set of cyber events affecting operational technology systems: those that are required to be reported to NERC, those that "cause interruptions of electrical system operations," and those that "could potentially impact electric power system adequacy or reliability."[4] In contrast, the NPRM would retain DOE Form DOE-417's broad applicability and significantly expand the reportable events to all substantial cyber incidents affecting operational technology system *and* information technology systems.

Second, the definition is redundant. Since all electric utilities must file DOE Form DOE-417 reports, including entities required to report to under NERC CIP standards is superfluous. All NERC CIP reporting entities are also DOE Form DOE-417 reporting entities. On its face, the NPRM's "covered

[3] The NPRM refers to the form by its previous designation, "OE-417."
[4] DOE OE-417 Instructions (Criteria for Filing #2, 3, 11, 14).

entities" definition appears to rely on well-established applicability requirements for the electric subsector, but indirectly the definition simply results in a meaningless sector-based criteria for the electric utility sector.

Third, including every electric utility in CIRCIA's reporting mandate is inconsistent with a risk-based approach to cybersecurity. Approximately 1,000 public power utilities serve fewer than 2,000 customers each, most of those serving fewer than 1,000 customers. These small, distribution-only utilities are essential to the small communities they serve but have virtually no impact on the reliability or security of the bulk power system. The Federal Energy Regulatory Commission (FERC) has repeatedly recognized the importance of a risk-based approach when approving NERC's CIP standards,[5] and it has properly imposed regulations—including incident reporting obligations—only on entities that pose a threat to the nation's critical infrastructure. By expanding the number of entities that must report *and* the type of incidents that must be reported *and* the amount of information to be reported, CISA may find itself receiving a lot of information about incidents that have little impact on national security.

APPA urges CISA to revise the definition of covered entities to exclude electric utilities that meet the Small Business Administration's thresholds for being a small business. Excluding small entities from the definition of covered entities has the dual benefit of (1) ensuring that entities with the highest risk profiles begin incident reporting immediately, thereby increasing national security; and (2) keeping the number of entities covered under the law to a limited, more manageable level, allowing CISA and industry to focus on the most significant threats.

B. CISA should execute a CIRCIA Agreement with electricity regulators *before* covered entities are required to begin reporting.

Congress was crystal clear that it did not intend for CIRCIA to result in duplicative reporting for critical infrastructure entities that already have mandatory requirements to report cyber incidents.[6] The NPRM states CISA's intent to abide by that principle, which APPA applauds. But it appears CISA is going forward with its rule without having finalized plans and agreements to implement that intent. The electric sector already has several mandatory and voluntary reporting requirements for cybersecurity incidents—most notably the NERC CIP standards and the DOE Form DOE-417 report—but CISA has not offered any explicit confirmation that it will deem those existing reporting requirements to be substantially similar to its proposed requirements.

While there are some differences between the NPRM's proposed reporting requirements and the existing reporting requirements for the electric sector, CISA should easily conclude that the existing reports are substantially similar, especially if CISA adopts the changes and clarifications proposed by APPA. APPA recognizes that entering into CIRCIA Agreements with DOE, FERC, and/or NERC (not to mention the agencies for other sectors) will take some time and may require some effort to ensure reporting

---

[5] *See, e.g., Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, P 35, *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016) ("We intend that NERC's proposed modifications will be designed to address the risk posed by the assets being protected in accordance with the risk-based approach reflected in the CIP version 5 Standards, *i.e.*, the modifications to address Low Impact BES Cyber Systems may be less stringent than the provisions that apply to Medium and High Impact Cyber Systems – commensurate with risk.").

[6] *See* 6 U.S.C. § 681f(a) (establishing the Cyber Incident Reporting Council to harmonize requirements); 16 U.S.C. § 681f(d) (requiring a report on duplicative reporting requirements); *see also* Dep't of Homeland Security, Harmonization of Cyber Incident Reporting to the Federal Government (Sept. 19, 2023).

obligations are indeed substantially similar. Nevertheless, it is essential that CISA complete those consultations and enter into the necessary agreements *before* finalizing the CIRCIA rule.

The NPRM states: "To the extent practicable, CISA is committed to working in good faith with its Federal partners to have CIRCIA Agreements finalized before the effective date of the final rule."[7] The NPRM further indicates that CISA aims to finalize the rule in late 2025 and make the reporting obligation effective in early 2026.[8] The NPRM is silent, however, on what will happen if CISA and its federal partners are unsuccessful in reaching agreement prior to the end of 2025.

APPA urges CISA not only to commit to good faith efforts to reach agreement with DOE, FERC, and NERC, but also to commit that if such agreement is not reached, CISA will delay the effective date of the CIRCIA rule for the electric sector. Without such a commitment, there is a risk that information sharing agreements will not be executed prior to the CIRCIA rule becoming mandatory on electric utilities, and the result will be duplicative reporting requirements contrary to Congressional intent.

C. CISA should facilitate a single reporting mechanism for all state and federal agencies that have voluntary or mandatory reporting of cyber incidents.

Electric utilities, including public power utilities, already make several separate reports to state and federal agencies in the aftermath of cyber incidents. As noted, NERC and DOE already have mandatory reporting requirements. Additionally, some public power utilities are required to report some cyber incidents pursuant to individual state laws on data security and data breach reporting. Outside of these mandatory reporting standards, public power utilities participate in robust voluntary information sharing systems, such as the Electricity Information Sharing and Analysis Center (including the E-ISAC CRISP program, in which some APPA members participate) and the Multi-State Information and Sharing Analysis Center, as well as the Cyber Mutual Assistance program established by the Electricity Subsector Coordinating Council. And, following a cyber incident, a public power utility will likely contact local *and* federal law enforcement agencies.

In short, there are far too many government agencies that need to be informed about a cyber incident in its immediate aftermath. And since federal agencies have limited ability to share information among themselves and even less ability to share information with state agencies, the burden of filing multiple reports falls on the owners and operators of critical infrastructure. The lack of interagency and intergovernmental coordination harms national security and safety because it draws industry resources away from the time-sensitive and critical task of responding to a cyber incident.

The implementation of CIRCIA is an opportunity for CISA to provide leadership in offering a single, streamlined reporting portal so that a covered entity could submit information in one place, and the website would then forward the relevant pieces of information to all state and federal agencies that have voluntary or mandatory reporting of cyber incidents. CISA's proposed user-friendly, dynamic, web-based portal for submitting reports can and should be expanded to be a platform through which covered entities can submit information once and be confident that the information will reach all relevant federal and state entities.

[7] NPRM, § III.D.
[8] NPRM, § V.A.i.

D. CISA should clarify that an electric utility's size is a relevant factor in determining whether an impact is substantial or serious.

The NPRM proposes to define a "substantial cyber incident" based on the impact the incident has on the covered entity. Impact 1 is a "*substantial* loss of confidentiality, integrity or availability of a covered entity's information system or network." And Impact 2 is a "*serious* impact on the safety and resiliency of a covered entity's operational systems and processes." The NPRM explains that whether an incident "is or is not a substantial cyber incident is fact-dependent and must be assessed on a case-by-case basis."[9] It further identifies factors that should be considered in determining whether a loss is substantial: "[the determination] will likely depend on a variety of factors, such as the type, volume, impact, and duration of the loss."[10]

APPA urges CISA to clarify that an electric utility's size is another relevant factor to be considered when determining whether a loss is substantial under Impact 1 or an impact is serious under Impact 2. Consider, for example, an attack that leads to a multi-day loss of availability of an electric utility's customer billing system. For a large electric utility with millions of customers, such a loss may be considered substantial; but for a small utility that only sends bills to its few hundred customers once a month, the same attack is likely not substantial.

APPA believes that—to the extent CISA fails to exclude small businesses from the definition of covered entities[11]—for small, distribution-only electric utilities, the only types of incidents that qualify as a substantial loss or serious impact under Impact 1 and Impact 2 are incidents that lead to an actual electrical outage.

Granting APPA's requested clarification is entirely consistent with the NPRM, which already acknowledges that determinations under Impact 1 and Impact 2 are fact-specific and are affected by a (non-exhaustive) list of a variety of factors. Granting clarification will also minimize the reporting burden on small entities, consistent with the goals of the Small Business Regulatory Enforcement Fairness Act of 1996.

E. CISA should clarify that, for electric utilities, a disruption of business or industrial operations refers only to a disruption of electricity generation or delivery.

Impact 3 under the NPRM's thresholds for identifying substantial cyber incidents is a "disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services."[12] Unlike the first two impacts, Impact 3 does not contain a qualifier such as 'substantial' or 'serious.' Thus, as proposed, *any* disruption to business or industrial operations or delivery of goods or services would qualify as a reportable incident.

APPA urges CISA to clarify that, with respect to the electric sector, Impact 3 refers only to a disruption of electricity production or delivery. Many electric utilities provide goods or services that are incidental to the delivery of electricity. For example, some utilities provide energy efficiency products or offer customer education services. A disruption to those incidental goods or services do not warrant a CIRCIA report, unless the impacts are substantial or serious under Impact 1 or Impact 2.

---

[9] NPRM, § IV.A.ii.3.a.i.
[10] *Id.*; *see also* § IV.A.ii.3.a.ii (listing similar factors for Impact 2).
[11] *See* Section A, *supra*.
[12] Proposed § 226.1.

Granting APPA's clarification is consistent with CIRCIA's goal of protecting *critical infrastructure*. Only disruptions affecting critical infrastructure are properly reportable under the statute.

F. CISA should clarify that it does not expect covered entities to provide all the required data about an incident in the initial reports provided within 24 of a ransom payment or 72 hours of a reportable cyber incident.

Proposed § 226.8 and § 226.9 require covered entities to provide, within 24 or 72 hours of an incident, more than two dozen types of information in a CIRCIA report. Some of that information will likely be readily available and can be provided immediately (e.g., the date the incident was detected, a brief description of the systems affected and the operational impacts, the amount of a ransom payment). But much of the required information is much more time consuming to provide. For example, it could take several months of forensic analysis with the support of law enforcement and expert consultants to identify "the tactics, techniques, and procedures used to perpetrate the covered cyber incident."[13] Even information that does not require forensic analysis—e.g. description of functions of affected networks and devices including technical details and physical locations—could take more than 24 hours to compile into a usable format for reporting.

APPA does not oppose the short timeline for submitting an initial CIRCIA report but urges CISA to clarify that it does not expect covered entities to provide all the required information in that initial report. Instead, covered entities should be expected to provide all readily available information in their initial reports, with the remainder of the required information to be provided in supplemental reports.

The NPRM recognizes that entities will supplement their initial reports as more information becomes available: Proposed § 226.11 allows for covered entities to submit supplemental reports that may include "information the covered entity was required to provide as part of a Covered Cyber Incident Report but did not have at the time of submission and information." But even that language implies that covered entities are 'required' to provide all the information in the initial report.

Granting this clarification is consistent with the statutory requirements while also ensuring that complying with CIRCIA's reporting obligations does not detract from restoring critical infrastructure. Covered entities must dedicate all their available resources in the hours following a cyber incident to mitigate and remediate the effects. Any technical subject-matter resources spared to collect information for reporting requirements are resources that are not being dedicated to remediating the incident.

G. CISA should clarify that the amount of preliminary analysis needed to form a reasonable belief that a covered cyber incident has occurred is fact specific.

CIRCIA requires covered entities to submit a report within 72 hours after the covered entity "reasonably believes" that a covered cyber incident has occurred. The NPRM properly acknowledges that forming a reasonable belief that a covered incident occurred "is subjective and will depend on the specific factual circumstances related to the particular incident."[14] The NPRM also properly recognizes that some preliminary analysis must be performed to establish reasonable belief. The NPRM, however, contradicts its subjective-and-fact-specific conclusion by stating "CISA believes that in most cases, this preliminary analysis should be relatively short in duration (i.e., hours, not days)" and "generally would occur at the subject matter expert level and not the executive officer level."[15]

---

[13] Proposed § 226.8(e).
[14] NPRM, § IV.E.iv.1.
[15] *Id.*

Public power utilities have a wide range of procedures for detecting, analyzing, and responding to cyber incidents. In larger organizations, for example, an incident response team is immediately formed upon detection of any *potential* incident, followed by well-defined roles for team members to investigate and follow a clear decision making and escalation framework. In such cases, a security officer may have responsibility for declaring that an incident has occurred. In smaller organizations, a utility employee may have to contact an external expert to analyze whether an anomaly is the result of a system error or an unlawful intrusion. Thus, the duration of the preliminary analysis and the seniority level at which it occurs cannot be generalized: it remains subjective and fact specific.

One particular example where it will often take longer to reach a reasonable belief that a covered cyber incident has occurred is for incidents that fall under Impact 4: unauthorized access caused by a third party.[16] Unlike the other prongs of the definition of covered cyber incidents, Impact 4 does not contain any qualifier such as 'substantial' or 'serious'; that is, *any* unauthorized access through a third party will be reportable. Furthermore, the other prongs require a covered entity only to assess the *impact* of the incident to determine whether it is reportable, while Impact 4 requires a covered entity to assess the *cause* of the incident. Preliminary analysis of the incident's cause is usually more complex and time consuming than analysis of its impact, so it will often take longer for a covered entity to form a reasonable belief that an Impact 4 covered incident has occurred.

APPA therefore urges CISA to (1) reaffirm its conclusion that reasonable belief is subjective and fact specific, and (2) acknowledge that Impact 4 covered incidents may be more time-consuming to identify.

H. Unsuccessful attempts are properly excluded from the definition of cyber incidents.

Proposed § 226.1 defines a cyber incident to mean an occurrence that "actually jeopardizes" an information system or the information on such a system. The NPRM explains that the definition excludes unsuccessful hacking attempts.[17] It goes on to give examples of activities that do not trigger a reporting obligation: blocked phishing attempts, failed attempts to gain access to systems, and routine scanning that presents no evidence of penetration.

APPA strongly supports this element of CISA's proposal. First, it follows Congress's clear instruction that an occurrence that "imminently, but not actually, jeopardizes" an information system is excluded from CIRCIA's reporting requirement.[18] Second, excluding attempted intrusions from the reporting requirement supports CISA's goal of detecting and countering sophisticated cyber campaigns by filtering out reports of the near constant stream of non-credible attacks that are routinely blocked by critical infrastructure entities. Finally, the exclusion properly minimizes the reporting burden on covered entities by avoiding unnecessary reports.

I. Penalties for false statements is appropriately limited.

Proposed § 226.20(a) provides that any person that "knowingly and willfully makes a materially false or fraudulent statement or representation" in connection with CIRCIA's reporting requirements is subject to

[16] NPRM, § IV.A.ii.3.a.iv ("Impact 4: Unauthorized Access Facilitated Through or Caused by a: (1) Compromise of a CSP, Managed Service Provider, or Other Third-Party Data Hosting Provider, or (2) Supply Chain Compromise").
[17] NPRM, § IV.A.ii.3.b ("if a cyber incident jeopardizes an entity or puts the entity at imminent risk of threshold impacts but does not actually result in any of the impacts included in the proposed definition, the cyber incident does not meet the definition of a substantial cyber incident.").
[18] 6 U.S.C. § 681(5); *see also* 6 U.S.C. § 681b(c)(2)(A).

penalties. The NPRM provides a safe harbor for entities that mistakenly submit inaccurate information and correct the information when the error is discovered.[19]

APPA supports limiting any potential penalties to knowing and willful misrepresentations and the explicit clarification that mistakes that are corrected are not considered false statements. Entities that make a good faith effort to provide timely information during complex and dynamic investigations into a cyber incident should not be subject to penalties.

J. State and federal freedom of information laws are properly preempted.

Congress explicitly exempted CIRCIA reports from disclosure under the federal Freedom of Information Act, as well as any similar state, tribal, or local freedom of information laws.[20] Proposed § 226.18(b)(2) properly codifies that exemption.

APPA supports this element of CISA's proposal. Many public power utilities are subject to state or local freedom of information laws, and some of those laws lack adequate exceptions for cyber security information related to critical electric systems. CIRCIA reports will almost always contain sensitive critical energy information that could be used by adversaries if publicized, so protecting that information from freedom of information laws will further Congress's objective of reducing the national security consequences associated cyber incidents.

[19] NPRM, § IV.G.vii ("CISA would not consider scenarios where a covered entity reports information that it reasonably believes to be true at the time of submission, but later learns through investigation that it was not correct and submits a Supplemental Report reflecting this new information, to constitute a false statement or representation.").
[20] 6 U.S.C. § 681e(b)(2).