Edison Electric INSTITUTE

Power by Association℠

COMMENTS OF THE EDISON ELECTRIC INSTITUTE ON THE DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S, PROPOSED RULE REGARDING CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE

89 Fed. Reg. 23,644
Docket No. CISA–2022–0010

The Edison Electric Institute (EEI) appreciates the opportunity to respond to the *Notice of Proposed Rulemaking*, entitled *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*, issued by the Cybersecurity and Infrastructure Security Agency (CISA) on April 4, 2024.[1] The NPRM's purpose is Twofold—(1) to put forth CISA's proposed regulations for implementing the requirements of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)[2] and (2) to provide interested persons an opportunity to submit written comments in response thereto.

Among other things, CIRCIA directs CISA to develop and oversee implementation of regulations requiring critical infrastructure entities (i.e., covered entities) to submit to CISA reports detailing covered cyber incidents and ransom payments. Under the Proposed Rule, covered entities will have 72 and 24 hours, respectively, to report to CISA a covered cyber incident and a ransom payment (even if it is not a payment associated with a covered

[1] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644 (proposed Apr. 4, 2024) (NPRM or Proposed Rule).
[2] 6 U.S.C. § 681 (Lexis 2024).

cyber incident), respectively. The Proposed Rule, if adopted in its current form, will substantially expand on existing U.S. cybersecurity incident reporting requirements and have important implications for how covered entities respond to cyber incidents. The Proposed Rule is designed to help federal authorities better coordinate critical infrastructure threat responses and share vital details with industry and government. CISA expects to publish a final rule by late 2025, with reporting likely beginning in 2026.

I. IDENTIFICATION OF FILING ENTITY

EEI is the association that represents all U.S. investor-owned electric companies, some of which also own and operate natural gas infrastructure. EEI member companies provide electricity to more than 250 million Americans and operate in all 50 states and the District of Columbia. The electric power industry supports more than seven million jobs in communities across the United States. EEI members are investing $150 billion annually to make the energy grid more secure against all hazards, including cybersecurity threats. The EEI member companies' approach to cybersecurity is driven by factors unique to their operational environment—including (but not limited to) their operational safety; regulatory requirements; affordability; and threat-informed, risk-based analysis.

II. INTRODUCTION

EEI and its members wholly endorse the policy objectives underpinning CIRCIA. CIRCIA is an important law, with an important goal of identifying cyber risk across all sectors of the economy. Critical infrastructure cybersecurity is a shared responsibility, and cyber incident reporting can help government and industry identify trends across sectors, leading to more effective policy making, information sharing, resource allocation, and mitigation strategies. EEI member companies appreciate and understand the shared

responsibility between private industry and our federal partners to secure the grid and are committed to working with both public and private partners, across all sectors, to comply with incident reporting requirements in a way that prioritizes and enhances critical infrastructure security.

That said, details matter when it comes to how CIRCIA, or how any mandatory cyber incident reporting regime, is implemented. A failure to properly identify, scrutinize, and address relevant details will ineluctably result in unintended negative consequences. These comments seek to elaborate on how the energy sector, along with our federal partners, can shape CISA's future incident reporting schema in a manner that avoids such unintended negative consequences and achieve CIRCIA's goals in the most effective way.

As currently drafted, the Proposed Rule will require extensive efforts by critical personnel during the most critical phase of an incident. When combined with a low threshold for reporting, this will impose significant burdens and compliance obligations on covered entities. Worse yet, it will do so during the most critically important time of a cyber incident—the initial hours/days of detection, which is when a compromised entity's resources, attention, and efforts are needed most to neutralize and mitigate the underlying threat.

CIRCIA is a new legal obligation that applies to one of the most difficult and sensitive times of an organization's cybersecurity program, response, and recovery. It sets legal rules of behavior in a constantly developing field. Thus, it risks burdening cybersecurity operations and flooding CISA with notifications. It is for these reasons that EEI and its members suggest narrowly tailoring terms under the Proposed Rule to allow all to gain experience with its application. Where proposed definitions and requirements are

unclear or may require interpretation, EEI and its members recommend erring on the side of clarity at the price of comprehensiveness: the focus should be on gathering quality information, not the quantity thereof. As all parties gain more experience in the actual application, CISA can update and recalibrate the rules accordingly.

When CIRCIA was enacted, Congress was careful to note the legislation sought to strike a balance between CISA receiving information quickly and the impacted entity responding to an attack without imposing burdensome requirements.[3] To illustrate, CIRCIA specifically defines "covered cyber incident[s]" as "substantial cyber incidents", not "all" or "any" cyber incidents.[4] On the contrary, the Proposed Rule would disrupt Congress' intended balance by suggesting that covered entities report on all cyber incidents and share sweeping investigative findings and details that are typically not available until weeks or months after an incident. Accordingly, CISA should refine its broad interpretation of the CIRCIA statute, including definitions and data requirements. Without more precise definitions and clear reporting thresholds, over or under reporting will occur, which could undermine the effectiveness of CIRCIA and potentially overwhelm industry and government resources.

Additionally, in its final rule, CISA should clarify how it will provide Sector Risk Management Agencies (SRMAs) with the information they need to fulfill their responsibilities and coordinate with entities in their respective sectors. EEI and its members

[3] *See e.g.*, Press Release, *Sen. Homeland Sec. and Gov't Affairs Comm., Portman, Peters Introduce Bipartisan Legislation Requiring Critical Infrastructure Entities to Report Cyberattacks* (Sep. 28, 2021), https://www.hsgac.senate.gov/media/reps/portman-peters-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyberattacks/.
[4] 6 U.S.C. § 681 (Lexis 2024).

would also like to see SRMAs utilized as entry points for critical sectors, rather than CISA trying to be all things to all sectors.

Furthermore, it is also important to underscore the CIRCIA partnership implies reciprocity. To fulfill CIRCIA's purpose, CISA should ensure it is adequately equipped to intake incident reports and has the capabilities and subject matter expertise to provide timely and actionable information back out to industry, along with tools to help minimize or avoid threats and support victims as they respond to highly debilitating attacks.

EEI and its members are committed to continuing to work with CISA to refine the Proposed Rule and ensure its successful implementation. If its requirements are balanced appropriately, CIRCIA will help reduce attacks and the disruption they cause to individuals, businesses, our economy, and our way of life.

CIRCIA's success rests on getting this final rule right.

III. RECOMMENDATIONS

For the reasons explained in the remainder of these comments *infra*, EEI and its members ask CISA to revise the Proposed Rule as follows:

- CISA should raise the impact thresholds in its proposed definition of "substantial cyber incident" in the manner proposed herein *infra* so that the criteria for what to report and when to report are focused on our national security posture or capabilities and ensure critical infrastructure entities are helped by the final rule and not further burdened or penalized by it.
- Any information required in the final rule to meet CIRCIA reporting requirements should be aligned with that which is already required in existing federal reporting standards. Moreover, CISA's data reporting requirements should be tailored to

sector-specific needs and focus only on data which can meaningfully inform analytical efforts to produce actionable information for the private sector. With respect to the energy sector, CISA should align its reporting requirements with Form DOE-417 for electric companies and TSA Security Directive Pipeline-2021-01D for natural gas pipelines.

- In order to make data retention manageable and reasonably cost effective, EEI and its members recommend that CISA significantly reduce the proposed amount of data required for preservation or the retention period, or both. In addition, the data-retention requirements promulgated in CISA's final rule should reflect an understanding that all information is not readily available due to technological and system constraints. The combination of the large volume of data covered entities would be required to retain and the two-year data preservation period would make this an unduly burdensome requirement, as the costs and related manpower required to maintain the necessary hardware and software and organize and audit the requested data would be substantial.
- CISA must do all it can to protect reported information from threat actors and recognize its own limitations. Specifically, CISA should establish a multi-layered approach to securing covered entity information in transit, storage, and use and provide visibility to covered entities regarding how this data will be managed and secured throughout its lifecycle.
- CISA should clarify it is proposing to interpret the term "promptly", as it relates to the required timeframe for submitting supplemental reports updating previously provided Covered Cyber Incident Reports, to mean "without delay or as soon as

possible", rather than within 24 hours of a covered entity's discovery of "substantial new or different information" compared to that which was included in its Covered Cyber Incident Report.

- CISA should provide greater clarity on the information protections afforded by a covered entity's decision to mark information as "Commercial, Financial, and Proprietary". CISA should also provide clarity on how such markings will inform CISA's decision to share information contained in CIRCIA Reports or responses to requests for information (RFIs), either with other federal departments or agencies or as part of the statutorily required reports in which CISA will document aggregated/anonymized findings, observations, and recommendations.
- Given the sensitivity of the information contained in CIRCIA Reports and RFI responses, CISA should develop and communicate a process for notifying covered entities when information contained in CIRCIA Reports or RFI responses is shared with other federal departments and agencies or when CISA receives similar reports from other federal departments and agencies.
- CISA should leverage the proposed "substantially similar reporting exception" in order to achieve cyber reporting harmonization to the maximum extent practicable, as per the Biden Administration's national harmonization mandate; to this same end, CISA should also put forward in its final rule a process or mechanism for maintaining harmonization with a federal agency counterparty under a CIRCIA Agreement terminated by CISA.

IV. EEI MEMBERS' COMMITMENT TO CYBERSECURITY

A. Energy, Particularly Electricity, Is Essential to Daily Life in the United States.

The electricity subsector is a part of the energy sector that is designated by National Security Memorandum/NSM-22 as one of the 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health and safety, or any combination thereof.[5] A reliable supply of electricity is key to supporting a strong national economy, as well as maintaining and preserving national security. The reliance of virtually all industries on electric power and natural gas means that all critical infrastructure sectors have some dependence on the energy sector.[6]

Energy, particularly electricity, is fundamental to public health, safety, and national security because it is a lifeline function that enables all other lifeline functions, including telecommunications, transportation, health care, and water. As an industry with critical infrastructure, the electric subsector employs a risk-based, defense-in-depth approach to cybersecurity, including employing a variety of tools and strategies that support existing voluntary and mandatory cybersecurity standards and regulations, both of which are valuable tools in ensuring the cybersecurity of critical infrastructure operators. Given the

[5] The White House, National Security Memorandum on Critical Infrastructure Security and Resilience, Daily Comp. Pres. Docs., 2024 DCPD No. 202400358 at 17-18 (Apr. 30, 2024) (National Security Memorandum or NSM-22).

[6] Cybersecurity and Infrastructure Security Agency, Critical Infrastructure Sectors: Energy Sector, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector (last visited Jul. 2, 2024).

criticality of electricity to all facets of Americans' daily lives, electric companies engage in thorough, systematic work to protect the Bulk Power System (BPS).

While CIRCIA is the first federal cybersecurity reporting requirement focused specifically on reporting across all 16 critical infrastructure sectors, electric and natural gas companies (electric companies, together with natural gas companies, collectively, energy companies) have been subject to similar reporting for years. Pursuant to mandates imposed by the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), the Transportation Security Administration (TSA), and the Department of Energy (DOE), respectively, energy companies are already subject to cybersecurity and incident reporting requirements that are intended to provide greater situational awareness to help energy companies and government protect and respond to cybersecurity incidents. These responsibilities and duties protect the grid and should be considered by CISA as it determines how to implement its own cybersecurity and incident reporting regulations.

B. Voluntary Partnerships Are Integral to EEI Members' Cybersecurity Defense Posture and Therefore Must Not Be Inimically Affected by the Reporting Requirements Put Forward in CISA's Final Rule.

In addition to complying with existing mandatory cybersecurity and incident reporting requirements, EEI member companies engage in voluntary partnerships that focus on threat and vulnerability sharing and use additional strategies and tools to mitigate cyber risk. These activities include regular exercises for a variety of emergency situations impacting the BPS, up to and including national-scale exercises, such as NERC's bi-annual GridEx. These exercises allow utilities to demonstrate how they would respond to and

recover from simulated coordinated cyber- and physical-security threats and incidents, strengthen their crisis communications relationships, and develop lessons learned.

Relatedly, the electric industry and its federal partners already invest significant resources in partnerships focused on addressing national security risk. For example, the CEO-led Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the electric power industry and its federal partners with respect to efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC works across the subsector, and with the Electricity Information Sharing and Analysis Center (E-ISAC), to develop actions and strategies that help protect the North American energy grid and prevent a spectrum of threats from disrupting electricity service. The ESCC includes CEOs and executives from electric companies, public power utilities, and rural electric cooperatives, as well as their trade association leaders, who represent all segments of the industry. Through the ESCC, the industry works closely with its federal partners, including senior administration officials from the White House, cabinet agencies, federal law enforcement, and national security organizations. Canadian electric company executives also are represented on the ESCC due to the international make-up of the North American energy grid.

CyberSentry is a CISA-managed threat detection and monitoring capability, governed by an agreement between CISA and voluntarily participating critical infrastructure partners who operate significant systems supporting National Critical Functions. CyberSentry monitors for both known and unknown malicious activity affecting information technology (IT) and operational technology (OT) networks. CISA's CyberSentry program enables trusted partnerships between CISA and each participating

critical infrastructure organization for mutual benefit and the benefit of critical infrastructure entities nationwide. The program's unique partnerships provide an added layer of defense for partners by securely leveraging sensitive government information and providing shared opportunity for visibility and mitigation of highly consequential cyber threats targeting critical infrastructure. Relevant insights gained from the program are used for the collective defense of infrastructure across partners and nationwide.

Building on the industry's culture of mutual assistance and informed by lessons learned from major destructive cyber incidents overseas as well as by exercises held in North America, the ESCC formed the Cyber Mutual Assistance (CMA) Program in 2016. The CMA Program is a natural extension of the electric power and natural gas industries' long-standing approach of sharing critical personnel and equipment when responding to emergencies. The CMA Program is comprised of industry cyber experts who can provide voluntary assistance to other participating entities in advance of, or in the event of, a disruption of electric or natural gas service, systems, IT infrastructure, or any combination thereof due to a cyber emergency. In addition, these cyber experts collaborate under the CMA Program framework to share information and conduct exercises. The CMA Program is one of the tools used by industry to enhance our nation's ability to defend and protect against threats and meet customers' expectations.

The Cybersecurity Risk Information Sharing Program (CRISP) is another example of the electric industry's ongoing voluntary coordination efforts with its federal partners to enhance cybersecurity. CRISP leverages advanced technology and industry expertise to provide its participants with near real-time delivery of relevant and actionable threat information regarding their IT networks. CRISP is a public-private partnership between

industry, the E-ISAC, and DOE. Data collected through CRISP is used to identify cyber-threat actors, pinpoint emerging trends, and analyze correlations across the energy sector. The bi-directional information sharing between electric companies and DOE enables CRISP analysts to develop a comprehensive cyber-threat landscape of the energy sector.

Finally, DOE's Cybersecurity Capability Maturity Model (C2M2) was the corollary of government and industry collaboration through an industry advisory group that was facilitated through a series of working sessions. The group incorporated feedback from more than 60 industry experts to create a descriptive, rather than prescriptive, model that helps organizations improve their cybersecurity capabilities. The model is flexible and therefore allows organizations to adapt it to their respective unique operational environments; as such, it accounts for electric companies' various structures, locations, functions, sizes, etc. The model is a useful voluntary framework for EEI members.

Through these partnerships, the expertise and innovation of both industry and our federal partners is harnessed to improve threat and vulnerability detection, analysis, and sharing capabilities. Significant resources from responsible entities and federal partners are engaged in these efforts. Common to these sharing partnerships is the fact that they are voluntary, based on trust, and focused on enhancing critical infrastructure cybersecurity. Many efficiencies can be gained in leveraging existing mandatory cybersecurity incident reporting requirements and voluntary partnerships. Accordingly, CISA's forthcoming cybersecurity information reporting requirements must not weaken the ability of EEI member companies to participate in these programs by shifting their focus to new compliance activity. Therefore, CISA should carefully consider the impacts its proposal may have on these partnerships when developing its proposed reporting requirements.

V. COMMENTS

A. CISA's Proposed Definition of "substantial cyber incident" Is Too Broad and Therefore Must Be Narrowed in Scope.

CIRCIA defines a "covered cyber incident" as a "substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established" by CISA.[7] As a result, CISA, in its NPRM, proposes to define the term "covered cyber incident" to mean a "substantial cyber incident".[8] Under the Proposed Rule, covered entities would be required to report a substantial cyber incident, which CISA propounds to define as a cyber incident meeting any of the following four requirements:

> (1) A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
>
> (2) A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
>
> (3) A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or
>
> (4) Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a:
>
> > (i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
> >
> > (ii) Supply chain compromise.

Proposed Rule, 89 Fed. Reg. 23,644, 23,767 (proposed Apr. 4, 2024). The scope of the third and fourth impact prongs of this proposed definition is overly broad because neither features a qualifier, such as "critical", "substantial", or "significant", whereas the first two impact prongs do. Without such a qualifier that limits prongs 3 and 4 to critical, serious, or

[7] 6 U.S.C. § 681b(c)(2)(A) (Lexis 2024).
[8] Proposed Rule, 89 Fed. Reg. 23,644, 23,766 (proposed Apr. 4, 2024).

substantial impacts, it is exceedingly difficult—if not impossible altogether—for a covered entity to know what would be excluded from the plain letter of this proposed definition and, in turn, would likely result in under and over reporting due to covered entities interpreting prongs 3 and 4 differently. The reason for this is because entities following the plain language of CISA's proposed definition will over report, creating large volumes of minor incident reports for CISA to sift through, while other entities will attach "substantial" to the third and fourth prong in alignment with Congressional intent.

To bring it into alignment with CIRCIA, EEI and its members recommend the following revisions to the NPRM's proposed definition of "substantial cyber incident":

> (1) A substantial loss of confidentiality, integrity, or availability of a Ceovered Eentity's information system or network;
>
> (2) A serious impact on the safety and resiliency of a Ceovered Eentity's operational systems and processes required for the provision of products or services by that entity;
>
> (3) A substantial disruption of a Ceovered Eentity's ability to engage in business or industrial operations required for the provision of products or services by that entity~~, or deliver goods or services~~; or
>
> (4) An unauthorized access with a substantial impact to a Ceovered Eentity or a substantial disruption of business or industrial operations due to a loss of service to a Ceovered Eentity's information system or network that is facilitated through or caused by a:
>
> > (i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
> >
> > (ii) Supply chain compromise.

(Note that the above definition capitalizes defined terms (e.g., "Covered Entity", "Substantial Cyber Incident"), which we recommend CISA do for all such terms in the

"Definitions" section and preamble of the final rule.) These recommended revisions will bring this definition into alignment with existing electric subsector reporting because this revised definition would include Form DOE-417 and NERC CIP-008 reporting if the incident results in a substantial operational disruption. "Substantial Cyber Incident[s]" would also include other events not required by DOE or NERC. Specifically, this recommended definition would include events that result in a substantial loss of confidentiality, integrity, or availability to an information system or network (e.g., business impacts with no operational impact). It also includes those that substantially disrupt a "Covered Entity['s]" ability to engage in business (e.g., an information system not related to electricity operation). Incidents facilitated or caused by a third party that result in an unauthorized access with a substantial impact to the "Covered Entity" (e.g., a vendor compromise that results in unauthorized access to the "Covered Entity['s]" employee records) or substantially disrupt the "Covered Entity['s]" business operations (e.g., a vendor compromise that results in that vendor being unable to perform an important business function for the Covered Entity) would also be in scope under this recommended definition.

CIRCIA requires that the final rule provide a "clear description of the types of substantial cyber incidents that constitute covered cyber incidents."[9] The Proposed Rule, however, lacks any such descriptions. Instead, CISA provides examples of incidents that "likely would qualify as substantial cyber incidents"[10] but then clearly explains that these examples are simply indicators of the "relative likelihood that such an incident would or

[9] 6 U.S.C. § 681b(c)(2)(A) (Lexis 2024).
[10] Proposed Rule, 89 Fed. Reg. 23,644, 23,668 (proposed Apr. 4, 2024).

would not rise to the level of a reportable substantial cyber incident."[11] In fact, CISA proposes that the actual determination of whether a cyber incident is a substantial cyber incident be made on a case-by-case basis specific to the circumstances, making understanding the requirements difficult for covered entities.[12] To account for this vague, case-by-case definition, which implies that only CISA can determine whether an incident is reportable, CISA encourages reporting all cyber incidents, thereby explaining CISA's proposed grossly excessive information reporting requirements.[13] However, this does not reflect the legislative intent behind CIRCIA, which according to one of its sponsors, Congresswoman Yvette Clarke (D-NY), was to establish "reporting requirements [that] would be appropriately tailored to limit overreporting and ensure that CIRCIA ultimately yields the security benefits that we intended."[14] Without clear guidance, covered entities will over or under report.

As further observed by Senator Portman (R-OH), when CIRCIA was enacted, Congress was careful to note "the legislation [sought] to strike[] a balance between getting information quickly and letting victims respond to an attack without imposing burdensome requirements."[15] EEI recognizes CIRCIA's requirement for covered entities to report substantial cyber incidents due to third-party- or supply-chain compromise; however, the Proposed Rule's definition of "substantial cyber incident" would disrupt that balance by

[11] *Id.*
[12] *Id.*
[13] *Id.* at 23,668 ("CISA continues to encourage reporting or sharing of information about all cyber incidents, even if it would not be required under the proposed regulations.").
[14] *Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking Before the Subcomm. on Cybersecurity and Infrastructure Protection of the House Homeland Sec. Comm.* (May 1, 2024 (opening statement of Rep. Clarke (D-NY)).
[15] Press Release, *U.S. Sen. Homeland Sec. Comm., Peters & Portman Landmark Provision Requiring Critical Infrastructure to Report Cyber-Attacks Signed into Law as Part of the Funding Bill* (Mar. 15, 2022), https://www.hsgac.senate.gov/media/dems/peters-and-portman-landmark-provision-requiring-critical-infrastructure-to-report-cyber-attacks-signed-into-law-as-part-of-funding-bill/.

requiring entities to report not just substantial cyber incidents but any incident that involves data loss or unauthorized access into an information system (e.g., a laptop). Accordingly, CISA should revise its definition of "substantial cyber incident" in the manner recommended herein to establish substantial impact thresholds. Specifically, the definition of "substantial cyber incident" should be revised to ensure a higher threshold for reporting and avoid over reporting of incidents that cause minimal harm or impact. Impact thresholds will allow CISA to focus on data elements that inform actionable intelligence and reduce the burden on covered entities.

Not all cyber incidents have the same level of severity and rise to the level of "substantial" that merits reporting. For example, an incident where a threat actor gains access but is not able to move beyond a single endpoint device would have little impact on the covered entity's business or operations, although the device user's ability to work is disrupted until the device is cleaned or replaced. These incidents are common; generally, quick to resolve; and often the result of phishing emails from compromised vendor email accounts. Conversely, another incident originating from a supply-chain compromise in which a threat actor is able to access a covered entity's laptop, move laterally, and gain control of an OT system is likely to have a significant impact. While these are important distinctions, the two incidents could look similar in the early stages of an investigation. Furthermore, consideration of the impact and severity of an incident is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures. Therefore, the more explicit CISA is in this definition, the fewer instances of over reporting or reporting incidents that do not have an impact on U.S.

economic and national security, as envisioned in the legislation.[16] This will help ensure that CISA receives the credible cyber incident data needed to capture actual incidents of national-level impact without imposing unnecessary additional burdens on entities reporting and responding to incidents in real-time.

Conversely, an overly broad definition of "substantial cyber incident" would present enormous compliance challenges for covered entities and create a deluge of reports that would make it difficult, if not impossible, for CISA to determine trends through "the noise". An overly broad definition would also result in covered entities diverting limited resources from strengthening information systems to regulatory reporting functions. It is a delicate balance. The criteria for what to report and when to report it should always be focused on our national security posture or capabilities and ensuring critical infrastructure entities are helped by the final rule and not further burdened or penalized by it.

In addition, when considering the reporting requirements of a supply-chain compromise, CISA should consider that a company affected by such a breach might not have all relevant data available for a complete report. Consequently, covered entities should only be required to disclose the information made available to them by the compromised vendor; CISA must also understand that covered entities may be limited in their disclosures based on contractual obligations and rights with the vendor (e.g., confidentiality obligations).

[16] 6 U.S.C. § 681(9) (Lexis 2024) (defining "Significant Cyber Incident" to mean "a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.").

B. The Amount of Information Required Under the Proposed Rule Is Excessive and Gratuitous, Significantly Increasing a Covered Entity's Reporting Burden While Often Contributing Little Analytical Value.

CIRCIA's reporting requirements are substantial in and of themselves, mandating the inclusion of six categories (and multiple subcategories) worth of information—by far the most copious of any current federal reporting requirement. Because these information reporting requirements are statutorily mandated, their inclusion in the final rule is compulsory. CISA, on the other hand, discretionarily proposes in its NPRM to greatly expand upon CIRCIA's already substantial information reporting requirements by mandating the inclusion of an additional 21 subcategories of information—none of which is required by CIRCIA. Many of these requirements lack a clear nexus to responding to cybersecurity incidents and, in doing so, conflict with Congress' clear intent in CIRCIA.

For example, the Proposed Rule would require covered entities to provide "the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found", "any controls or measures that resulted in the detection or mitigation of the incident", and "a description and a copy or samples of any malicious software the covered entity believes is connected with the covered cyber incident" in addition to the CIRCIA requirements.[17] By contrast, CIRCIA only requires a "description of the vulnerabilities exploited and the security defenses that were in place, and the tactics, techniques, and procedures used to perpetrate the incident."[18] Likewise, it is unclear how requiring a covered entity to disclose any entity that it requested assistance from in

[17] Proposed Rule, 89 Fed. Reg. 23,644, 23,771 (proposed Apr. 4, 2024) (creating 6 C.F.R. §§ 226.8(c),(d), and (g).
[18] 6 U.S.C. § 681b(c)(4)(B) (Lexis 2024).

responding to a cyber incident or ransomware incident will aid overall incident response,[19] much less be worth the expenditure of covered entities' resources required to compile and submit this information to CISA.

In total, the sheer breadth and volume of information CISA proposes to require for CIRCIA reporting is so inordinately excessive it would overburden covered entities and CISA, while, in some cases, providing CISA with very little analytical value. Covered entities do not have the personnel or required resources to identify, extract, and produce this much data, especially as they try to respond to and recover from a cyber incident. Anything CISA proposes to add to the statutory requirements of CIRCIA is simply another layer on top of already burdensome reporting requirements across various jurisdictions and sectors and should therefore be removed from the final rule. Again, CISA is the authority tasked with harmonizing federal cybersecurity incident reporting requirements. Accordingly, any information required in the final rule to meet CIRCIA reporting requirements should be aligned with that which is already required in existing federal reporting standards, as opposed to layering on additional complexity.

Excessive reporting requirements create burdens on covered entities responding to incidents, diverting resources to reporting rather than securing their systems. This is due to the entirety of personnel required for accurate reporting are directly involved in the response process as well. While an energy company's response team naturally prioritizes tactical response, many of the same resources will be involved in emergency response operations as well in instances when operations or customers, or both, are impacted. The level of detail specified by CIRCIA takes days or weeks to uncover and document and may

[19] Proposed Rule, 89 Fed. Reg. 23,644, 23,771-72 (proposed Apr. 4, 2024) (creating 6 C.F.R. §§ 226.8(i)(4) and 226.9(i)(4)).

require the use of additional resources (i.e., retained services). Therefore, when a covered entity must leverage personnel to prioritize compiling evidence and transmitting reports, they are taking away from the resources available to restore impacted systems to an operational state. In addition to exceeding the clear direction provided in CIRCIA, encouraging reporting of all cyber incidents is not reasonable in light of existing information sharing programs such as those enumerated and delineated previously herein *supra* (e.g., CyberSentry, CMA, and CRISP).

Relatedly, CISA's data reporting requirements should be tailored to sector-specific needs and focus only on data which can meaningfully inform analytical efforts to produce actionable information for the private sector. With respect to the energy sector, EEI and its members recommend CISA, in the final rule, align its reporting requirements with Form DOE-417[20] for electric companies and with TSA Security Directive Pipeline-2021-01D for natural gas companies.[21] Otherwise, energy companies will be forced to navigate a

[20] Form DOE-417 requires respondents to report on the event and actions taken to resolve the incident—including, as appropriate, the cause of the incident or disturbance, change in frequency, mitigation actions taken, the equipment damaged, critical infrastructure interrupted, effects on other systems, and preliminary results from any investigations. Respondents must also identify the estimated restoration date, the name of any lost high-voltage substations or switchyards, whether there was any electrical system separation (and if there were, what the islanding boundaries were), and the name of the generators and voltage lines that were lost (shown by capacity type and voltage size grouping), as well as Cyber Attributes for cyber events-including the functional impact, the attack vector used, and the level of intrusion that was achieved or attempted. *See* Form DOE-417, Electric Emergency Incident and Disturbance Report 3, https://www.oe.netl.doe.gov/docs/OE417FormInstructions05312024.pdf.

[21] TSA Security Directive Pipeline-2021-01D requires owner/operators to include the following information, as available to the reporting owner/operator at the time of the report (1) the name of the reporting individual and contact information, including a telephone number or email address (the report must also explicitly specify that the information is being reported in order to satisfy the reporting requirements in this Security Directive); (2) the affected hazardous liquid and natural gas pipeline(s) and/or facilities, including identifying information and location; (3) a description of the threat, incident, or activity, to include a) information about who has been notified and what action has been taken; b) any relevant information observed or collected by the owner/operator, such as malicious IP addresses, malicious domains, malware hashes and/or samples, or the abuse of legitimate software or accounts; and c) any known threat information, to include information about the source of the threat or attack, if available; (4) a description of the incident's impact or potential impact on information or operational technology systems and operations; this information must also include an assessment of actual, imminent or potential service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding

reporting environment where under-resourced security professionals must consult a Venn diagram of reporting obligations to comply with conflicting regulations, taking time away from actual threat-response activities. Should CISA, in its analysis, identify a need to augment the information available through a revised, streamlined list of required data points, it may leverage its provided RFI authorities or simply reach out to the covered entity, in coordination with DOE (i.e., the energy sector SRMA), as needed to supplement the reported information.

Significantly scaling back and streamlining with existing federal reporting requirements will also ensure CISA receives useful information, rather than a lot of "signal", and better enable it to pinpoint those incidents and threat factors that are really of the most significance; moreover, it will provide CISA the ability to very quicky turn that back around so that if a financial institution, for example, is experiencing something that might come to face an electric or a telecom company, such information can be propagated very quickly to critical infrastructure entities and relevant federal agencies to forestall further spread of the identified threat. If CISA does not take the time to thoughtfully streamline the information required for CIRCIA reporting to a manageable set of data, the resulting information reporting requirements put forth in the final rule will simply add to the burden of an already overburdened set of professionals, as opposed to improve and strengthen America's cybersecurity posture. To avoid such unintended negative consequences, data reporting requirements should be limited to include only information that is necessary to facilitate the spirit of the law, which is to provide rapid response in

the impact or potential impact of the cybersecurity incident; and (5) a description of all responses that are planned or under consideration, to include, for example, a reversion to manual backups, if applicable. *See* Security Directive Pipeline-2021-01D at 3-4 (TSA Security Directive Pipeline-2021-01D), (May 29, 20243), https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01d.pdf.

times of triage (i.e., significant incidents) so that CISA can help victims, forewarn other critical infrastructure entities in the ecosystem, and integrate, assemble, study, and analyze the information, as well as produce mitigating communications—all in an effort to help avert other attacks.

C. CISA Must Do All It Can to Protect Reported Information from Threat Actors and Recognize Its Own Limitations.

CIRCIA ultimately aims to improve situational awareness of cybersecurity threats in order to improve the nation's cybersecurity posture. However, CISA reported that it was the target of a cybersecurity intrusion by a malicious actor from January 23, 2024, to January 26, 2024, and that information in the Chemical Security Assessment Tool (CSAT) could have been inappropriately accessed.[22] This recent attack highlights the challenges with protecting such a high-value target and underscores our adversaries' interest in collecting such information.

Drawing a parallel to CISA's Proposed Rule, a compromise of the information CISA collects under CIRCIA reporting could have severe consequences for national security due in part to the size and inherently critical nature of the critical infrastructure entities regulated under CIRCIA. CIRCIA Reports require highly sensitive information on items that would be extremely valuable to threat actors. For example, the "technical details and physical locations" of every system involved in a cybersecurity incident[23] becomes so

[22] Greig, Jonathan and Smalley, Suzanne, *CISA Forced to Take Two Systems Offline Last Month After Ivanti Compromise*, The Record (Mar. 8, 2024), https://therecord.media/cisa-takes-two-systems-offline-following-ivanti-compromise (noting that a CISA spokesperson confirmed that CISA "identified activity indicating the exploitation of vulnerabilities in Ivanti products the agency uses" and reporting that the systems involved included the CSAT, which houses private-sector chemical security plans).

[23] Proposed Rule, 89 Fed. Reg. 23,644, 23,770-71 (proposed Apr. 4, 2024) (creating 6 C.F.R. §§ 226.8(a)(1)(i) and 226.9(a)(1)(i)).

specific that the utility to CISA is eclipsed by the risk of consolidating such information for numerous critical infrastructure operators across all sectors into one target.

Given CISA's recent cyber incident that impacted its CSAT portal, industry is rightfully concerned about the consolidation of extremely sensitive information from all critical infrastructure sectors in one place that is managed by an agency which just experienced a compromise of extremely sensitive information. As such, EEI and its members request that CISA reconsider the amount of information it will collect and require covered entities to preserve. Narrowing the thresholds for reporting triggers as well as reducing the volume of required information is necessary to make this reporting regime a net-positive for the nation's cybersecurity. No security is foolproof, not even CISA's; therefore, aggregating this highly sensitive information in one place creates unnecessary risk for covered entities, CISA, and the nation. CISA should consider at what point collecting the "technical details and physical locations" of every system involved in a cybersecurity incident[24] becomes so specific that the utility for incident response is eclipsed by the risk of consolidating such information for numerous critical infrastructure operators across all sectors into one target.

For these reasons, EEI members urge CISA to establish a multi-layered approach to securing covered entity information, not just by limiting the potential impact by reducing the volume of sensitive data, but by employing the requisite leading practices for protecting this data in transit, storage, and use. It is essential that CISA responsibly provides increased visibility to covered entities regarding how this data will be managed and secured through its lifecycle, including the agency's hiring plans, use of artificial intelligence, and

[24] Proposed Rule, 89 Fed. Reg. 23,644, 23,770-71 (proposed Apr. 4, 2024) (creating 6 C.F.R. §§ 226.8(a)(1)(i) and 226.9(a)(1)(i)).

anticipated costs to attract and retain the top-tier level of skilled workforce needed to protect covered entity information.

D. The Proposed Rule's Data-Preservation Requirements Are Unduly Onerous.

As currently proposed in the NPRM, regardless of whether a covered entity submits a CIRCIA Report or is eligible for an exception from reporting, it must preserve data and records related to the covered incident or ransom payment for no less than two years from the date of submission or the date the submission would have been required.[25] Covered entities that submit CIRCIA Reports would be required to begin preserving the prescribed data at the earlier of either (a) the date upon which the entity establishes a "reasonable belief" that a covered cyber incident has occurred, or (b) the date upon which a ransom payment was disbursed.[26] A covered entity would also have to preserve the data for a period of no less than two years from the submission of the latest required CIRCIA Report submitted pursuant to the Proposed Rule, to include any supplemental reports.[27] This data-preservation requirement would attach to data and records relating to communications between the covered entity and the threat actor; indicators of compromise; relevant log entries, memory captures, and forensic images; network information or traffic related to the cyber incident; the attack vector; system information that may help identify vulnerabilities that were exploited to perpetrate the incident; information on any exfiltrated data; data and records related to any ransom payment made; and any forensic or other reports about the cyber incident produced or procured by the covered entity.[28] A covered

[25] Proposed Rule, 89 Fed. Reg. 23,644, 23,731 (proposed Apr. 4, 2024).
[26] *Id.*
[27] *Id.*
[28] *Id.*

entity is not, however, required to create any data or records it does not already have in its possession based on this regulatory requirement.[29] The requirement for a covered entity to preserve data or records applies only to the extent the entity already has created, or would be creating them, irrespective of CIRCIA.[30] Of note, CIRCIA does not prescribe either the length of the data-retention period or the types/categories of data that must be preserved, leaving CISA the necessary tractability to prescribe both in an unduly burdensome manner.

EEI members' concerns regarding the data-preservation requirements outlined in the NPRM are not specific to the proposed length of time, per se; nonetheless, they are problematic in at least two respects. For one thing, these proposed requirements fail to make allowances for the technical feasibility of retaining the types/categories of data identified in these proposed provisions. For example, covered entities may not have the logs for some of the required data, in which case the length of time CISA requires an entity to retain such data is irrelevant. Accordingly, when it comes to data retention, the requirements put forward in CISA's final rule should reflect an understanding that all information is not readily available due to technological and system constraints.

Furthermore, the combination of the large volume of data covered entities would be required to retain and the two-year data preservation period would make this an unwieldy requirement, as the costs and related manpower required to maintain the necessary hardware and software and organize and audit the requested data would be substantial. Data retention is resource intensive and significantly burdensome; preserving voluminous amounts of data for protracted periods of time—as would be required under the NPRM's data-preservation requirements—greatly exacerbates this onus by placing an

[29] *Id.*
[30] *Id.*

ungainly burden on the resources that would be needed from a digital perspective and the workforce required to manage all of that data. Moreover, it raises significant questions. For instance, how do you manage two-years worth of that data? How do you manipulate it? How do you resource it? How do you have staff that deals with it? And how do you have the digital infrastructure that can actually maintain all of that data? Consequently, in order to make data retention manageable and reasonably cost effective, EEI and its members recommend that CISA significantly reduce the amount of data required for preservation or the retention period, or both.

E. The NPRM Proposes Separate Contrasting Interpretations of the Term "Promptly" as It Relates to the Timeframe Within Which Covered Entities Must Submit Supplemental Reports Updating Previously Submitted Covered Cyber Incident Reports.

Under section 681b(a)(3) of CIRCIA, a covered entity that has previously submitted a Covered Cyber Incident Report must ''promptly'', which is undefined in CIRCIA, submit to CISA an update or supplement to that report upon the occurrence of either of the following triggering events: (a) ''substantial new or different information becomes available'' or (b) ''the covered entity makes a ransom payment after submitting a covered cyber incident report.''[31] While the Proposed Rule does not put forward a definition for "promptly", CISA propounds two disparate/conflicting interpretations of this term with respect to the submission deadline for supplemental reports that update or supplement a previously submitted Covered Cyber Incident Report.

Specifically, during its discussion in the preamble regarding reporting exceptions, CISA states it proposes to interpret "promptly" to mean within 24 hours of the triggering event for the submission of all supplemental reports—meaning, covered entities would be

[31] 6 U.S.C. § 681b(a)(3) (Lexis 2024).

required to provide these reports to CISA within 24 hours of (i) discovering "substantial new or different information" than that which was included in their Covered Cyber Incident Report or (ii) following the remittance of a ransom payment.[32] However, in a different discussion in the preamble wherein it addresses the interpretation of "promptly" as it relates to the submission deadline for supplemental reports upon the occurrence of either of the two identified triggering events, CISA effectively provides two different interpretations of the term. One announces a 24-hour submission deadline for supplemental reports that is expressly limited to ransom payments that are made following a covered entity's submission of a Covered Cyber Incident Report.[33] And the other, which is not expressly limited to either of the triggering events, simply states "CISA interprets 'promptly' to generally mean what it means colloquially, i.e., without delay or as soon as possible."[34] Again, because CISA, in this same discussion, expressly proposes to interpret "promptly" to mean 24 hours for supplemental reports precipitated by ransom payments, CISA's concomitant interpretation (provided in this same discussion in the preamble) of "promptly" as meaning "without delay or as soon as possible" seemingly is wholly germane to the submission of supplemental reports that update or supplement previously submitted Covered Cyber Incident Reports (and are therefore unrelated to ransom payments). Otherwise, that language would be devoid of meaning. However, because CISA fails to state as much in its NPRM and provides in the previously referenced unrelated discussion earlier on in the preamble that it interprets "promptly" to mean "within 24 hours of the triggering event",[35] it is unclear whether CISA is proposing to interpret "promptly"

[32] Proposed Rule, 89 Fed. Reg. 23,644, 23,709-10 (proposed Apr. 4, 2024).
[33] *Id.* at 23,726.
[34] *Id.*
[35] *Id.* at 23,709-10.

to mean (i) "without delay or as soon as possible"[36] or (ii) "within 24 hours of the triggering event"[37] as the submission deadline for supplemental reports updating or supplementing previously submitted Covered Cyber Incident Reports.

Accordingly, with respect to supplemental reports that are unrelated to (and not precipitated by) ransom payments, EEI and its members request that CISA clarify in its final rule that it is interpreting "promptly" to mean "without delay or as soon as possible", rather than within 24 hours of discovering "substantial new or different information" than that which was included in their Covered Cyber Incident Report.[38] A 24-hour reporting requirement for supplemental reports updating previously filed Covered Cyber Incident Reports would simply be unworkable for EEI members, as they will need sufficient time to identify, triage, analyze, extract, and report any "substantial new or different" information that becomes available for inclusion in these reports.[39] Depending on the volume or complexity of such information, this process can take days or weeks to complete, not 24 hours.

F. CISA's Proposed Marking Requirement Needs Clarifying.

Under section 226.18(b)(2) of the Proposed Rule, all information submitted in CIRCIA Reports or RFI responses would be exempt from automatic disclosure under FOIA, regardless of whether or not it is marked "Commercial, Financial, and Proprietary Information".[40] However, the NPRM, through proposed section

[36] *Id.* at 23,726.
[37] *Id.* at 23,709-10.
[38] *Id.* at 23,726.
[39] *Id.*
[40] *Id.* at 23,775 (creating 6 C.F.R. § 226.18(b)(2)).

226.18(b)(1), concomitantly puts forward a process by which entities can mark information as "Commercial, Financial, and Proprietary Information".[41]

CISA should provide greater clarity on the information protections afforded by a covered entity's decision to mark information as "Commercial, Financial, or Proprietary". CISA should also provide clarity on how such markings will inform CISA's decision to share information contained in CIRCIA Reports or RFI responses, either with other federal departments or agencies or as part of the statutorily required reports in which CISA will document aggregated/anonymized findings, observations, and recommendations. Further, given the sensitivity of the information contained in CIRCIA Reports or RFI responses, CISA should develop and communicate a process for notifying covered entities when information contained in CIRCIA Reports or RFI responses is shared with other federal departments and agencies or when CISA receives similar reports from other federal departments and agencies.

G. Harmonizing Existing and Proposed Cybersecurity Requirements Is Vital.

Harmonization will help to ensure that (1) agencies receive the most helpful information and (2) covered entities are not unnecessarily overburdened by overlapping reporting requirements. Harmonization avoids duplication and will make certain that covered entities are not encumbered by reporting different information to different agencies, especially in the middle of a substantial cyber incident crisis. Decreasing the onus on covered entities—entities that will be focused on mitigating an attack and its aftermath—will mean that covered entities can focus their attention on responding to an attack rather than getting bogged down responding to various regulatory regimes that ask

[41] *Id.* (creating 6 C.F.R. § 226.18(b)(1)).

for different information in different formats. Harmonization will also avoid confusion and make sharing information more efficient and less burdensome for the government.

1. Cybersecurity reporting harmonization has been a point of emphasis for this Administration.

The Biden Administration has assiduously stressed the importance of harmonizing federal cyber incident reporting requirements. Strategic Objective 1.1 of the National Cybersecurity Strategy directs regulators to "work together to minimize…harms" in those instances in which "[f]ederal regulations are in conflict, duplicative, or overly burdensome" and "to harmonize not only regulations and rules, but also assessments and audits of regulated entities."[42] To this end, Objective 1.1 tasks the "[Office of National Cyber Director], in coordination with the Office of Management and Budget (OMB), [to] lead the Administration's efforts on cybersecurity regulatory harmonization."[43] Pursuant to this directive, on August 16, 2023, the Office of the National Cyber Director (ONCD) issued a Request for Information seeking "public comments on opportunities for and obstacles to harmonizing cybersecurity regulations, per Strategic Objective 1.1 of the National Cybersecurity Strategy."[44] In its September 2023 report entitled "Harmonization of Cyber Incident Reporting to the Federal Government", DHS acknowledged that companies are subject to a "patchwork of regulations and statutory authorities, many with unique and potentially overlapping information requirements, timelines, and submission methods."[45] To address this issue, DHS recommended that agencies harmonize cyber-incident reporting

[42] National Cybersecurity Strategy 9 (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[43] *Id.*
[44] Office of the National Cyber Director Request for Information, 88 Fed. Reg. 55,694 (Aug. 16, 2023).
[45] Department of Homeland Security, Harmonization of Cyber Incident Reporting to the Federal Government 4 (Sep. 19, 2023), https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.

requirements, streamline reporting processes, and reduce current and future regulatory burdens imposed on reporting entities.[46] Similarly, in CIRCIA, Congress established a Cyber Incident Reporting Council (CIRC) "to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulation."[47] Congressional leaders from both parties have urged the "harmoniz[ation of] existing cyber incident reporting requirements for the energy sector with CISA's forthcoming reporting requirements in order to provide clarity and consistency."[48] And, most recently, the Administration reaffirmed its commitment to harmonization in NSM-22, wherein it states, among other things, "the National Cyber Director, in coordination with the Director of the Office of Management and Budget, shall lead my Administration's efforts for cybersecurity regulatory harmonization with respect to security and resilience requirements, of which portions of the effort outlined in this memorandum are an essential component."[49]

For these reasons, EEI and its members appreciate CISA's recognition and acknowledgement of the fact that "covered entities may be subject to multiple, potentially duplicative requirements to report cyber incidents" and are heartened by CISA's express commitment "to exploring ways to harmonize this regulation with other existing Federal reporting regimes, where practicable".[50] As noted in the National Cybersecurity Strategy, "[e]ffective regulations minimize the cost and burden of compliance, enabling

[46] *Id.* at 25.
[47] 6 U.S.C. Code § 681f(a) (Lexis 2024).
[48] Letter from Sen. Joe Manchin, Sen. John Barrasso, Rep. Frank Pallone, and Rep. Cathy McMorris Rogers to Jennifer Granholm, Sec. of Energy (Apr. 8, 2022), https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/documents/April%208%202022%20Bicameral%20Letter%20to%20Granholm.pdf.
[49] NSM-22, Daily Comp. Pres. Docs., 2024 DCPD No. 202400358, at 11 (Apr. 30, 2024).
[50] Proposed Rule, 89 Fed. Reg. 23,644, 23,653 (proposed Apr. 4, 2024).

organizations to invest resources in building resilience and defending their systems and assets."[51] In contrast, inconsistent regulations add to electric companies' already high operational costs and misdirect limited resources and personnel from their core obligation—namely, to provide safe, reliable, and affordable service to their customers.

2. EEI Members Are Already Subject to Multiple Cybersecurity and Incident Reporting Requirements.

EEI members are regulated across their diverse operational environments at the federal level (e.g., electric utilities (FERC), natural gas pipelines (FERC, TSA, Department of Transportation), dams (FERC), and nuclear (Nuclear Regulatory Commission)); they are also subject to extensive state regulation. In addition, new federal cybersecurity and incident reporting requirements are being introduced into various government contracts, such as by the Coast Guard and military bases. Cybersecurity and incident reporting requirements are among the many regulations to which EEI members are currently subjected and therefore must comply. Specifically, FERC/NERC, TSA, and DOE each impose cybersecurity incident reporting requirements on energy companies. A brief overview of these respective federal reporting requirements follows.

a) FERC/NERC cybersecurity and incident reporting requirements

NERC's Reliability Standards and Critical Infrastructure Protection Reliability Standards (hereinafter Reliability Standards and CIP Reliability Standards, respectively) are promulgated by NERC; approved by FERC; and enforced by FERC, NERC, and

[51] National Cybersecurity Strategy 9 (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

NERC's Regional Entities. They apply to owners, operators, and users of the Bulk Electric System (BES).

NERC's CIP Reliability Standards are designed to address physical and cybersecurity risks. CIP Reliability Standards "implement a defense-in-depth approach to protecting the security of the BES Cyber System at all impact levels."[52] Moreover, "the CIP Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems."[53] CIP Reliability Standards allow EEI members the flexibility to tailor their risk management approaches. As FERC has recognized, this flexibility is important to accommodate the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risks."[54]

NERC cybersecurity standard CIP 008-6 stipulates the following requirements: (1) entities must implement one or more processes to identify and respond timely to security incidents; (2) the roles and responsibilities of the security incident response personnel must be clearly defined; (3) procedures for handling security incidents must be documented; (4) incident response plans must be tested once every 15 months; (5) incident reports must be retained to optimize future responses; and (6) following the testing of an incident response event, a covered entity should document learnings, update its existing response plan, and disseminate findings to the security team. This Standard also requires applicable facility owners to provide an initial notification to the E-ISAC and CISA's National Cybersecurity

[52] Federal Energy Regulatory Commission, *Commission Information Collection Activities (FERC-725B(5))*; *Comment Request; Extension* at 6, Docket No. RD23-3-000 (March 24, 2023).
[53] *Id.* at 6-7.
[54] Federal Energy Regulatory Commission, *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050, ¶ 44 (July 21, 2016).

and Communications Center within one hour after the determination of a Reportable Cyber Security Incident and by the end of the next calendar day after determining that a Cyber Security Incident was an attempt to compromise an applicable system.

b) TSA Security Directive Pipeline-2021-01D Reporting Requirements

Many EEI members own and operate electric infrastructure as well as natural gas infrastructure and are therefore subject to cybersecurity and reporting requirements through TSA. TSA Security Directive Pipeline-2021-01D,[55] applicable to owners and operators of critical hazardous liquid and natural gas pipeline infrastructure (owner/operators) notified by TSA that their pipeline system or facility is critical, is an update to TSA Security Directive Pipeline-2021-01C [56] —the first of two security directives issued by TSA to enhance the cybersecurity of critical pipeline systems in response to the Colonial Pipeline attack on May 7, 2021. TSA Security Directive Pipeline-2021-01D requires covered owner/operators to: (1) report cybersecurity incidents to CISA within 24 hours of identification; (2) appoint a cybersecurity coordinator and alternate to be available 24/7 to coordinate with TSA and CISA; and (3) conduct a self-assessment of cybersecurity practices, identify any gaps, and develop a plan and timeline for remediation.[57]

[55] Security Directive Pipeline-2021-01D 1 (TSA Security Directive Pipeline-2021-01D), (May 29, 2024), https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01d.pdf.
[56] Security Directive Pipeline-2021-01C 3 (TSA Security Directive Pipeline-2021-01C), (May 29, 2023), https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01c.pdf.
[57] TSA Security Directive Pipeline-2021-01D, (May 29, 2024), https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01d.pdf.

c) DOE Cyber Incident Reporting Requirements

DOE, through its Electric Emergency Incident and Disturbance Report (Form DOE-417), requires Electric Utilities, Balancing Authorities, and certain Generating Entities to report to DOE cyber events that cause "interruptions of electrical system operations" or "could potentially impact electric power system adequacy or reliability."[58] Prior to submitting the form to DOE via the online DOE-417 system, respondents are given a choice whether to share information collected on the DOE-417 form with NERC, the E-ISAC, or CISA.[59] Depending on the nature of the situation, this form must be filed either within one hour; six hours; by the end of the next calendar day after a determination of an attempted cyber compromise; or by the later of 24 hours after the recognition of the incident or by the end of the next business day of the incident.[60] DOE uses the information to fulfill its overall national security and other energy emergency management responsibilities, as well as for analytical purposes.

d) Federal Government Contracting Requirements

Many utilities today provide services to the federal government which put them in-scope for a number of contractual cybersecurity requirements implemented through the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS). Many of these federal government contracts additionally have incident reporting requirements of their own. For example, DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting", requires

[58] DOE-417, Electric Emergency Incident and Disturbance Report 2 (Form DOE-417), https://www.oe.netl.doe.gov/docs/OE417FormInstructions05312024.pdf.
[59] *Id.* at 3.
[60] *Id.* at 2.

certain incidents to be reported within 72 hours.[61] Others have been proposed which would apply to utilities as well, such as the Coast Guard's recently proposed cybersecurity rules[62] as well as the FAR amendments proposed by the Department of Defense, General Services Administration, and National Aeronautics and Space Administration on October 3, 2023.[63]

3. EEI and Its Members Strongly Urge CISA to Harmonize Its Proposed Reporting Requirements with Both Current and Future Federal Reporting Requirements.

As enumerated and delineated above, energy companies are already required to comply with extensive cybersecurity reporting requirements, each of which set forth different directives and timelines than those proposed in CISA's NPRM. If implemented, CISA's proposed regulations would result in new, duplicative, and contrasting reporting requirements and timelines vis-à-vis extant energy sector federal reporting mandates. Commendably, CISA, in its NPRM, expressly acknowledges that its proposed regulations would impose an additional reporting obligation upon electric companies that are already required to report to multiple federal agencies and states 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 both 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.

[61] Safeguarding Covered Defense Information and Cyber Incident Reporting, 48 C.F.R. § 252.204-7012 (a)(2) (Lexis 2024).
[62] Cybersecurity in the Marine Transportation System, 89 Fed. Reg. 13,404 (proposed Feb. 22, 2024).
[63] Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing, 88 Fed. Reg. 68,055 (proposed Oct. 3, 2023).

Proposed Rule, 89 Fed. Reg. 23,644, 23,689 (proposed Apr. 4, 2024). Likewise, CISA also commits to work with TSA, to the extent practicable, "to formalize the ability to comply with CIRCIA and TSA cyber incident reporting requirements through the submission of a single cyber incident report."[64]

While EEI members appreciate CISA's express commitments to harmonize its proposed reporting regulations with existing federal reporting requirements governing energy companies and to use its suggested "substantially similar reporting exception" to facilitate its efforts in this regard, the currently recommended triggering requirements for this exception are problematic in at least one critical respect. If unaddressed, this deficiency would severely limit—if not forestall altogether—its applicability and, in turn, effectively thwart CISA's harmonization efforts.

Specifically, under the propounded "substantially similar reporting exception", a covered entity that is required "by law, regulation, or contract" to report "substantially similar information" on a covered cyber incident or ransom payment to another federal agency in a "substantially similar timeframe" as that required under CIRCIA would not have to submit a CIRCIA Report.[65] This exception is expressly authorized by CIRCIA, and the foregoing informational and temporal conditions are prescribed by that statute as well.[66] Importantly, neither CISA nor CIRCIA define "substantially similar information", which gives CISA an extremely wide berth to leverage its harmonization efforts through an expansive application of this exception. However, in pulling the curtain back regarding how it plans to determine the

[64] Proposed Rule, 89 Fed. Reg. 23,644, 23,700 (proposed Apr. 4, 2024).
[65] *Id.* at 23,708.
[66] 6 U.S.C. § 681b(a)(5)(B) (Lexis 2024).

applicability of this exception, CISA appears to be poised to do the exact opposite. Specifically, CISA states:

> CISA's determination that information is substantially similar will hinge on whether the data and information required to be submitted in a CIRCIA Report form are substantively included in the report to the other federal agency.
>
> ****
>
> CISA will consider whether 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. CISA views functionally equivalent as meaning that the information or data serves the same function or use, provides the same insights or conclusions, and enables the same analysis as the information or data requested in the relevant CIRCIA Report form fields.

Proposed Rule, 89 Fed. Reg. 23,644, 23,709 (proposed Apr. 4, 2024). In other words, CISA proposes to limit this exception exclusively to those instances in which another federal agency requires the same volume and type(s) of reporting as CIRCIA. However, the breadth and scope of reporting prescribed under CIRCIA far outstrips that required by other federal agencies, rendering it impossible for information reported under other federal requirements to be found "substantially similar" to that required for CIRCIA reporting based on CISA's proposed narrow interpretation of that phrase. Consequently, as currently proposed, it would be a veritable impossibility for the "substantially similar reporting exception" to be met.

The NPRM holds out this exception as the primary—if not lone—mechanism CISA will use to effect harmonization.[67] Consequently, an intractable application and implementation of this exception will short-circuit any such efforts, which would be incongruous with CISA's express commitment to harmonize its proposed regulations

[67] Proposed Rule, 89 Fed. Reg. 23,644, 23,654 (proposed Apr. 4, 2024).

with other federal reporting requirements and antithetical to the Biden Administration's harmonization edict. Accordingly, CISA should construe the "substantial similarity" requirement flexibly in order to achieve CIRCIA's goal of effecting harmonization and ensuring that cyber incidents are reported to the federal government in a manner and timeframe that will allow CISA to fulfill its mission of protecting critical infrastructure, while avoiding duplicative reporting obligations and deferring to the expertise of sector-specific federal agencies.[68]

EEI members are also concerned about another aspect of CISA's recommended implementation of the proposed "substantially similar reporting exception". To be more specific, CISA proposes to enter into an information sharing agreement, which it suggests to call a "CIRCIA Agreement", with federal agencies that "receive[] cyber incident reports from one or more CIRCIA covered entities pursuant to a legal, regulatory, or contractual obligation" in instances in which the other federal agency's "reporting obligation requires submission of substantially similar information in a substantially similar timeframe" as CISA.[69] CISA concomitantly proposes to provide itself the ability to terminate any such CIRCIA Agreement at any time and for any reason.[70] Yet, it fails to propose a means by which to maintain harmonization with the federal-agency counterparty in those instances in which it decides to unilaterally terminate a CIRCIA Agreement. EEI and its members request that CISA, in its final rule, provide a means for maintaining harmonization in such instances.

---

[68] *See Chevron, U.S.A., Inc. v. NRDC, Inc.*, 467 U.S. 837, 865-66 (1984) ("[I]t is entirely appropriate for [administrative agencies] to …resolv[e] competing interests which Congress itself either inadvertently did not resolve, or intentionally left to be resolved by the agency charged with the administration of the statute in light of everyday realities.").

[69] Proposed Rule, 89 Fed. Reg. 23,644, 23,708 (proposed Apr. 4, 2024).

[70] *Id.* at 23,709 ("CISA may terminate a CIRCIA Agreement at any time as long as doing so would not violate any aspect of the agreement itself.").

VI. CONCLUSION

Once again, EEI and its members appreciate the opportunity to comment on the Proposed Rule and look forward to working with CISA on ensuring the contours of its final rule are informed and circumscribed by CIRCIA's policy goals. Questions on these comments may be directed to Travis Smith, Associate General Counsel, Reliability and Security (tsmith@eei.org | 202-508-5145) or David Batz, Managing Director, Cyber and Infrastructure Security (dbatz@eei.org | 202-508-5586).

Respectfully submitted,

/s/ Travis R. Smith, Sr.

Travis R. Smith, Sr.
Associate General Counsel, Reliability and Security
202.508.5145
tsmith@eei.org

David Batz
Managing Partner, Cyber & Infrastructure Security
202.508.5586
dbatz@eei.org

Edison Electric Institute
701 Pennsylvania Ave., N.W.
Washington, DC 20004

July 3, 2024