Before the
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Capitol Heights, MD 20743

In the Matter of	)	
	)	
Proposed Rule - Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements	)	Docket No. CISA-2022-0010
	)	RIN: 1670-AA04
	)	
	)	

COMMENTS

The American Gas Association (AGA), the Interstate Natural Gas Association of America (INGAA), the American Petroleum Institute (API), and the American Public Gas Association (APGA) herein collectively referred to as "Commenters," submit these comments pursuant to the *Proposed Rule* released April 4, 2024.[1]

I. SUMMARY

In the *Proposed Rule*, the Cybersecurity and Infrastructure Security Agency (CISA) sought comment on issues related to the implementation of the Cyber Incident Reporting for Critical Infrastructure (CIRCIA) reporting requirements. The Commenters have reviewed the *Proposed Rule* and provide the following comments for CISA to consider in finalizing the rule.

Commenters applaud CISA for its focus on cybersecurity events that **actually jeopardize** systems. To maximize the utility of the CIRCIA program, Commenters ask that CISA:

- Continue to focus only on those incidents that would **actually jeopardize** operations and clarify the definition of a "*substantial cyber incident*,"

[1] *See* Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644 – 23,776 (Apr. 4, 2024) ("*Proposed Rule*").

- Reduce the amount and refine the type of information to be reported in the first 72 hours,
- Reassess the assignment of responsibility for incident reporting along the supply chain,
- Reduce the amount and refine the kinds of information that must be retained by the entity,
- Minimize duplicative reporting requirements, and
- Ensure the security of the information being provided throughout the CIRCIA reporting process.

Commenters specifically urge CISA to consider focusing the information required to be reported in the first 72 hours on the following:

- The impact of the incident and its severity (to determine threat level and risk),
- The estimated timeline of the incident – specifically, when the attack is believed to have started, and
- The indicators of compromise as seen on the actually jeopardized system.

Commenters provide additional background and detail below on their recommendations. We appreciate CISA's time in considering these comments.

II. BACKGROUND

A. THE COMMENTERS

The American Gas Association, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 78 million residential, commercial, and industrial natural gas customers in the U.S., of which 95 percent—more than 74 million customers—receive their gas from AGA members. Today, natural gas meets one-third of the United States' energy needs. Natural gas utilities work collaboratively with CISA and the Transportation Security Administration (TSA), the pipeline sector's security regulator, to protect and defend critical infrastructure systems from cyber threats.

INGAA is a trade association that advocates the regulatory and legislative positions of importance to the interstate natural gas pipeline industry in the U.S. INGAA's 27 members represent the majority of interstate natural gas transmission pipeline companies in the U.S. INGAA's members, which operate approximately 200,000 miles of interstate natural gas pipelines, serve as an indispensable link between natural gas producers and consumers.

The American Petroleum Institute (API) represents all segments of America's natural gas and oil industry, which supports more than 11 million U.S. jobs. API's nearly 600 members produce, process, and distribute the majority of the nation's energy.

The American Public Gas Association (APGA) is the trade association representing more than 730 communities across the U.S. that own and operate their retail gas distribution entities. These include not-for-profit gas distribution systems owned by municipalities and other local government entities, all accountable to the citizens they serve.

B. CURRENT & EXPECTED PIPELINE SECURITY RULEMAKING

All of the Commenters' members are dedicated to securing the operations of their systems, engaging in a variety of voluntary frameworks, and participating in robust public partnerships, including with the multiple Sector Risk Management Agencies (SRMAs) as follows:

- The Department of Energy through the Oil and Natural Gas Subsector Coordinating Council (ONG SCC), and
- The Department of Homeland Security (DHS) through the Pipeline Modal SCC, the Maritime Modal SCC, and the Chemical SCC.

As such, we are actively engaged in all aspects of federal government activities and initiatives encompassing all hazards to promote the security and safety of critical infrastructure systems.

In 2021, Colonial Pipeline suffered a significant *ransomware attack* that caused the company to shut down its operations. In response to that event, several agencies have incorporated

lessons-learned from the Colonial Pipeline incident into sector regulations and guidance that continue to harden oil and natural gas cyber defenses and minimize opportunities for successful system compromise. Recently, the U.S. Coast Guard issued a Notice of Proposed Rulemaking for Marine Transportation Systems in addition to the White House's actions to bolster port security.[2] In issuing these regulations, the Coast Guard clarified that it was setting minimum standards designed to prevent future disruptions like the Colonial Pipeline incident. This includes implementing account security measures and requiring multifactor authentication processes, as well as conducting cybersecurity assessments and auditing cybersecurity plans. Several provisions of the latest regulation reflect the same principles incorporated by TSA in the first iteration of the second Security Directive described below.

TSA issued two Security Directives to bolster the security of critical pipeline systems: Security Directive Pipeline 2021-01 and Security Directive Pipeline 2021-02 in response to the Colonial Pipeline incident. Both Security Directives have been subsequently amended and updated to accommodate for feedback from the industry and changes in the cyberthreat landscape.[3] Through the Security Directives and the subsequent amendments in the series, pipeline owner/operators are subject to several ongoing reporting and assessment requirements specific to the risk portfolio of pipeline systems. Commenters' members are actively securing their networks in line with these requirements and will continue to share information with the federal government through these existing channels. Commenters' members will continue to collaborate with the federal government on securing critical networks and information sharing through the rulemaking

[2] Cybersecurity in the Marine Transportation System, 89 Fed. Reg. 13,404-514 (Apr. 22, 2024), https://www.federalregister.gov/documents/2024/02/22/2024-03075/cybersecurity-in-the-marine-transportation-system; *Fact Sheet: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports*, WHITE HOUSE (Feb. 21, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/.

[3] *See* Ratification of Security Directives, 88 Fed. Reg. 36,919-36,921 (June 6, 2023).

process. Furthermore, the Security Directives will soon be replaced by cybersecurity regulation for the surface transportation sector to include oil and natural gas.

Some pipeline operators were also required to comply with the Chemical Facility Anti-Terrorism Standards (CFATS) when the program was active. Should the program be reauthorized, as CISA suggests in the *Proposed Rule*,[4] operators owning facilities with chemicals of interest (COI) that meet or exceed screening threshold quantities will adopt and maintain security plans to deter the weaponization of these chemicals. In protecting systems from malicious actors, the CFATS incorporates cybersecurity standards and incident reporting practices.[5] The security plans required under CFATS, if reauthorized, address cybersecurity explicitly and ask that facilities list all their cyber systems, describe the measures to protect these systems, and provide reporting protocols for cyber incidents.

III. COMMENTERS RECOMMEND CISA FOCUS ON ONLY THOSE SUBSTANTIAL CYBER INCIDENTS THAT "ACTUALLY JEOPARDIZE" OPERATIONS

Commenters appreciate that CISA focuses the covered cyber incidents on those that are "substantial." As stressed in the legislation itself, the *cyber incident* should jeopardize *information systems* and "does not include an occurrence that imminently, but not actually, jeopardizes" *information systems*.[6] The *Proposed Rule* clarifies that a *cyber incident* is an incident that **actually jeopardizes**, without lawful authority, the integrity, confidentiality, or availability of information on an *information system* or actually jeopardizes, without authority, an *information system*. Carrying this focus on cyber events that **actually jeopardize** systems forward, the *Proposed Rule*

[4] *Proposed Rule* at 23,650.

[5] *See* CHEMICAL FACILITY ANTI-TERRORISM STANDARDS: REPORTING CYBER INCIDENTS, CISA, https://www.cisa.gov/sites/default/files/publications/fs_cfats-cyber-reporting-508.pdf.

[6] 6 U.S.C. § 681(5).

targets covered *cyber incidents* that are substantial, defined as incidents that result in any one of the following outcomes:

1. A substantial loss of confidentiality, integrity or availability of a *covered entity*'s *information system* or network (emphasis added);
2. A serious impact on the safety and resilience of a *covered entity*'s operational systems and processes (emphasis added);
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 either a compromise of a *cloud service provider*, *managed service provider*, other third-party data hosting provider, or a *supply chain compromise*.

All these impacts are to be read in line with events that **actually jeopardize** an entity's systems, as required by statute. While Commenters appreciate the definitions provided in the *Proposed Rule*, we seek clarification on the interpretation of the impact-based test for determining if a *cyber incident* that **actually jeopardizes** the *information system* is "substantial." Commenters encourage CISA to refer to definitions of a "*significant cyber incident*" as described in PPD-41[7] and refer to the Cyber Incident Severity Schema as described in Annex C of the National Cyber Incident Response Plan.[8]

[7] PRESIDENTIAL POLICY DIRECTIVE/PPD-41, THE WHITE HOUSE (July 26, 2016) ("A cyber incident that is (or group of related cyber incidents that together are) 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 American people"), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[8] NATIONAL CYBER INCIDENT RESPONSE PLAN, CISA (DEC. 2016), https://www.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

Further, Commenters recommend that supply chain access be clarified to mean access that actually jeopardizes the *information system* in relation to the scale and nature of the *covered entity*'s operations—such as an access that would lead to a substantial loss (noted under the first impact). Given how extensive a *covered entity*'s supply chain may be, unauthorized access within the supply chain is, unless further defined, overly broad. Commenters are concerned that the language as written would lead to over reporting and include non-relevant incidents as the language confuses whether the impact is truly one that would **actually jeopardize** the system.

For example, as Commenters understand the mission of the legislation, there may be situations where a website impact does not disrupt operations for the Commenters' members. Since the system itself was not affected, the incident should not need to be reported. Commenters are concerned that without further clarification, and a stricter focus on incidents that "actually jeopardize" operations, the operator would be preoccupied with reporting incidents that on a risk-scale would have minimal significance. Commenters recommend that CISA target only those operations that **actually jeopardize** an *information system* and not those that may cause disruptions to tangential networks but not place *information systems* in "actual jeopardy." In order to clarify this definition, Commenters suggest that the definition of "significant" be linked to the Cyber Incident Severity Schema. For example, Level 3 (High Orange) includes those incidents that are likely to result in a "demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence."[9] Interruptions in critical infrastructure operations and ability to serve the public need would often meet the Level 3 incident level. Linking the impacts under the significant *cyber incident* definition to a risk-based outcome would help scale the reporting to the entity's operations as well.

[9] *Id.* at 40.

Commenters recommendations and requests for clarity would help entities more easily identify when an incident is "significant" and to be reported. These recommendations would also achieve Congressional objectives for the legislation. As noted by Chairman Mark Green of the House Homeland Security Committee, the final CIRCIA rule will achieve its goal of ensuring "shared visibility of *substantial cyber incidents*" (emphasis added) without "imposing undue regulatory burdens[s]."[10] Commenters recommendations to focus on those events that **actually jeopardize** the systems, as clarified in existing documents like PPD-41, will "strike the balance" to create a proactive reporting regime that meets the needs of U.S. national security.

IV. COMMENTERS RECOMMEND CISA REDUCE AND REFINE THE AMOUNT OF INFORMATION REQUIRED IN INITIAL REPORTS

Commenters have several concerns about the reporting timeline and requirements which its members will be subject to, in addition to the other agency reporting schedules governing the Commenters' members. The volume of information that must be collected for the preliminary report and provided to CISA within 72 hours risks the member's ability to respond to the incident itself. Commenters are concerned that even requirements such as "a description of the *covered entity*'s security defenses in place" (emphasis added) would require so much detail, and is such a broad descriptor, that the owners/operators will spend much of the 72 hours providing a narrative account of their defense systems rather than succinctly providing the necessary information to CISA to be able to properly share cyber threat information to protect other systems from compromise. The Office of the National Cyber Director received information from commenters that the Chief Information Security Officers of their organizations spent 30-50% of their time not

[10] Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking: Hearing Before the Comm. of Homeland Sec., 118 Cong. (2024), https://homeland.house.gov/hearing/surveying-circia-sector-perspectives-on-the-notice-of-proposed-rulemaking/.

on security, but on compliance efforts[11]—far too much time when each minute responding to an incident is critical. Considering that owners/operators will need to use this limited 72 hours to collect as much information as they can, determine the federal regulatory schemes with which they must comply, work with partners along the supply chain as necessary, and report back to CISA, CISA should reduce the amount of information required in the first 72 hours following an incident to **only the most pertinent information**. Commenters believe that the information requested within the first 72 hours following an incident should address only the following:

- The impact of the incident and its severity (to determine threat level and risk),
- The estimated timeline of the incident – specifically, when the attack is believed to have started, and
- The indicators of compromise as seen on their system.

Commenters further suggest that CISA consider phased reporting requirements that would specify the kinds of information CISA requires between the first 72 hours and the *supplemental reports* as the entity uncovers relevant information. A staggered reporting approach would assist CISA as well by allowing CISA staff the appropriate time to review and analyze the information as they receive it. Commenters have valid concerns that the amount of information being requested by CISA would overwhelm its staff and put an undue burden on already-limited government resources.[12] Instead, the owner/operator of the critical infrastructure system can provide an initial

[11] *Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information*, OFF. OF THE NAT'L CYBER DIR. (June 2024), 1, 5 ("many sector chief information security officers report spending 30 to upwards of 50 percent of their time on regulatory compliance"), https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.

[12] *See* GOV'T. ACCOUNTABILITY OFF., CYBERSECURITY: IMPROVEMENTS NEEDED IN ADDRESSING RISKS TO OPERATIONAL TECHNOLOGY (MAR. 7, 2024), https://www.gao.gov/products/gao-24-106576. (noting that CISA has insufficient staff at present). As cybersecurity workforce challenges affect both the public and private sector, commenters would like to be sensitive to the workload they are imposing on both of their staffs through this compliance effort.

report within 72 hours of the most salient information and provide other requisite information over time, either through specific phased reporting timelines or supplemental reporting as information becomes available, for the CISA staff to review.

Should CISA decide to not adopt a phased supplemental reporting schedule, Commenters would agree that *supplemental reports* should be submitted "promptly" as in "without delay."[13] This would allow for the entity to report accurate information in a timely manner while dedicating attention and focus to mitigating and recovering from the event without fear of penalization.

Commenters want to confirm the understanding of the term "promptly." In the *Proposed Rule*, CISA notes that for the purposes of the "substantially similar" exception for *supplemental report*, "promptly" may mean within 24 hours of the triggering incident.[14] This directly conflicts with the original definition provided for in the *Proposed Rule* as the colloquial use of the term, to mean "without delay." Commenters ask for confirmation that "prompt" supplemental reporting will balance the need for information with the need for the entity to respond to the incident by focusing the term "promptly" to mean "without delay," rather than a fixed-24-hour period.

Commenters want to note that refining the amount of information to be produced within the first 72 hours combined with narrowing the scope of covered incidents, as discussed in Section III, will help reduce the overall amount of sensitive data held by CISA. Commenters are concerned the aggregation of the volume and type of information required to be submitted will make CISA an attractive target for malicious actors seeking to access critical infrastructure vulnerabilities. Recently, CISA was subject to a breach through the Ivanti products vulnerability, which enabled

[13] *Proposed Rule* at 23,726.
[14] *Id.* 23,710.

cyber actors to access the Chemical Security Assessment Tool (CSAT).[15] CISA has retained large amounts of critical and sensitive data submitted originally under CFATS through the CSAT, including security vulnerability assessments and chemical security plans. While CFATS has been inactive since July 2023, the data collected during the program's operations and retained by CISA to date remains relevant and vital to system security—leaving many owners/operators concerned about the information that may have been accessed during this recent breach. Further, while CISA investigations suggested no evidence of data exfiltration, there also exists no evidence that sensitive data was not taken other ways (e.g., screenshots). Given that CIRCIA will increase the amount of sensitive information to be held by CISA, Commenters suggest CISA adopt additional measures to secure the data collected. These proposals are outlined in Section VIII of these comments.

V. COMMENTERS RECOMMEND CISA REASSESS THE ASSIGNMENT OF RESPONSIBILITY FOR INCIDENT REPORTING ALONG THE SUPPLY CHAIN

Regarding Impact 3 under the *Proposed Rule,* Commenters agree with CISA that reporting requirements should consider cascading impacts along the supply chain; however, the responsibility of reporting should be placed primarily on the entity who suffered the *cyber incident*. The CIRCIA guidelines provide examples of Impact 3, including "where a critical access hospital is unable to operate due to a *ransomware attack* on a third-party medical records software company on whom the critical access hospital relies; the critical access hospital, and perhaps the medical records software company as well if it also is a *covered entity*, would need to report the incident."[16] CISA will want to be informed of this event in order to achieve its objectives and secure the

[15] Jonathan Greig & Suzanne Smalley, *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.

[16] *Proposed Rule* at 23,663.

nation's infrastructure ecosystems. However, Commenters recommend CISA not require covered entities serving as customers to the supply chain carry the responsibility of reporting under this provision; it will be largely ineffective given customers will not have the same access to critical information relating to the incident as the affected entity. For example, a Commenter's member will not be able to provide several elements required under Section 226.8, including the below information:

- Descriptions of the unauthorized access, if the unauthorized access occurred on the third-party's system or network.
- Descriptions of the vulnerabilities exploited and the security defenses that were in place by the third-party.
- Descriptions the tactics, techniques, and procedures (TTPs) used to perpetrate the incident on the third-party's system or network.
- The identifying or contact information related to each actor reasonably believed to be responsible for the incident.
- The technical details and physical locations of networks, devices and/or *information systems* that were, or are reasonably believed to have been affected.
- A description of any unauthorized access (to the third-party), regardless of whether the incident involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed (by the third-party).
- The timeline of compromised system communications with other (third-party) systems.
- For covered *cyber incidents* involving unauthorized access (to third-party systems), the suspected duration of the unauthorized access prior to detection and reporting.

- A description of the (third-party's) security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the incident.
- Any indicators of compromise observed in connection with the covered *cyber incident*.
- A description of any mitigation and response activities taken by the (third-party) in response to the covered *cyber incident*, including but not limited to: (1) identification of the current phase of the (third-party's) incident response efforts at the time of reporting; (2) the (third-party's) assessment of the effectiveness of response efforts in mitigating and responding to the covered *cyber incident*; and (3) identification of any law enforcement agency that is engaged in responding to the covered *cyber incident*.
- Whether the (third-party) requested assistance from another entity in responding to the incident and, if so, the identity of each entity and a description of the type of assistance requested or received from each entity.

Because Commenters' members would not have access to information regarding the nature of the *cyber incident* and the security protocols used by the affected vendor, the reports submitted by the operator in this scenario would be incomplete and not advance the objective of the *Proposed Rule*. Commenters recommend that CISA focus on the third-party entity(ies) that have critical information. CISA is strongly encouraged to adopt the following proposals to improve the efficacy and efficiency of the CIRCIA program in the Impact 3 scenario:

First, Commenters propose that CISA continue to include third-party cybersecurity incident reporting within the scope of the CIRCIA regulation, so the affected entity is providing CISA with the most up-to-date and accurate information to understand cybersecurity breach trends, current threats, and the overall risk landscape.

Second, Commenters recommend that CISA modify the requirements for third-party cybersecurity incident reporting in the final rule. Commenters believe that owners/operators of critical infrastructure systems should only be responsible for reporting their system impacts and not that of their third-party vendors or partners. The reporting requirements and responsibilities in a third-party situation, as described by the example under Impact 3 listed above, should take into consideration required reporting entities along the supply chain will have limited information to share. This also applies to organizations (e.g., trade associations) that support owners/operators. Commenters recommend that owners/operators be held to reporting the following information when concerning a third-party cybersecurity incident:

- Owner/operator contact information.
- Owner/operator date of official notification of the third-party cybersecurity incident from the third-party that was the target of the incident.
- The name of the third-party organization that was targeted by the incident.
- If possible, the contact information for the third-party organization's point-of-contact.
- The name and brief description of the third-party system that was compromised in the incident.
- Whether or not the owner/operator experienced any operational impact, and if so, a brief description of the impact and high-level financial estimate of the impact.
- Owner's/operator's date of official notification that the third-party cybersecurity incident was officially closed and all outstanding cybersecurity remediations and mitigations were completed by the third-party. Alternatively, use the date the owner/operator decided to remove the

third-party's system from use and sever all connections to the third-party's compromised system and/or environment.

The information listed above is more likely to be within the scope of information shared with the owner/operator of a critical infrastructure system at the time of the third party's incident. Further, it should be sufficient information to provide CISA with notice that the incident occurred and to support it with the information needed to pursue further investigation. Commenters encourage CISA to work collaboratively with the third party, which was the target of the attack, rather than speaking solely to the owner/operator of critical infrastructure.

Finally, Commenters propose CISA provide accommodations to covered entities to forgo reporting if doing so would violate standing confidentiality agreements or other regulations unless the *covered entity* or the third party believes there is a threat of death, serious bodily harm, or serous economic harm.[17] The owner/operator of the critical infrastructure system impacted by the incident may have entered into Non-Disclosure Agreements or Confidentiality Agreements with its seller or other entities that would prohibit it from disclosing information to CISA. This accommodation is tailored to ensure that the objectives of the *Proposed Rule* are met, while allowing for entities to ensure that they do not violate any existing contracts in complying with CISA.

Further, CISA should work directly with federal agencies who employ confidentiality schemes to establish methods for sharing critical information directly between the agencies. The burden, as noted in comments on the harmonization efforts in Section VII of these comments, should rest on the government who has the authority and information to handle such reconciliation

[17] As interpreted by CISA, serious economic harm includes a terrorist act or use of a weapon of mass destruction. *Proposed Rule* at 23,739 n.389.

efforts rather than on the individual covered entities who are subject to third-party contracting terms. For example, entities may have standing agreements with the Department of Energy's (DOE) Cybersecurity Risk Information Sharing Program (CRISP) which would prevent the *covered entity* from sharing certain information with CISA even when required under the CIRCIA final rule. In establishing the reporting requirements for customers under Impact 3, CISA should consider instituting a final rule that protects the owner/operator from liability to the third party if, and when, the owner/operator discloses any information it has access to relevant to the incident.

VI. COMMENTERS RECOMMEND CISA REDUCE AND REFINE THE KINDS OF DATA REQUIRED TO BE RETAINED BY COVERED ENTITIES TO MITIGATE THE BURDEN ON REPORTING ENTITIES

Section 226.13 of the *Proposed Rule* requires covered entities to retain data and records related to the *substantial cyber incident* for two years following the conclusion of the event and final report. Retaining the vast amounts of data relating to an incident for the timeline suggested in the *Proposed Rule* places a significant cost and resource burden on the *covered entity*. According to the *Proposed Rule,* the final report is only to be submitted to CISA when there is a good faith belief that "further investigation would not uncover any substantial new or different information about the covered *cyber incident*."[18] It may take months or years for the investigation to meet the definitions of "conclusion,"[19] during which time the *covered entity* will continue to review, analyze, and evaluate the cause and nature of the incident. Throughout this investigatory period, the *Proposed Rule* directs the *covered entity* to retain all relevant, or potentially relevant, information associated with the incident. Commenters are concerned that given the long

[18] *Proposed Rule* at 23,724.

[19] *Id.* at 23,727 ("Although the point at which an incident is concluded and fully mitigated and resolved may vary based on the specific facts of the incident, reaching the following milestones is a good indication that an incident has been concluded and fully mitigated and resolved: (1) the entity has completed an investigation of the incident, gathered all necessary information, and documented all relevant aspects of the incident; and (2) the entity has completed steps required to address the root cause of the incident").

investigatory timeline and the two-year retention period following a final report (should one be issued) the *covered entity* may be required to retain large amounts of data for several years. Further, CISA notes that information which may seem insignificant at first, could become relevant later,[20] meaning that covered entities may be overly broad in their retention policies to maintain any item that could be of relevance, regardless of likelihood. In reviewing the *Proposed Rule*, Commenters note that the retention requirements may require its members to store up to 6 terabytes of data a day—storing these huge swaths of data will incur additional expenses and require significant workforce commitments to manage. The *Proposed Rule* does not seem to appropriately consider the requirements and its associated costs – especially if the *covered entity* was to report multiple incidents over multiple years. Commenters recommend that CISA expressly clarifies the type and quantity of data that must be preserved and the length of time for which such data must be preserved, and CISA reassesses the resources (financial and human) associated with storage as well.

Commenters further recommend CISA refine the amount of information needing to be retained for the two years following the issuance of a final report. Specifically, CISA should allow for summaries of findings or documents to be retained in place of original copies, as currently required under Section 226.13. Allowing for descriptions of the original documents would allow covered entities to reduce the volume of data being stored on their systems for extended periods of time. Commenters also recommend that following the final report, CISA should permit entities to remove any information that was deemed unrelated, or likely to not be relevant, at the time of the final report from their systems. As the investigations are completed, the likelihood that a previously unidentified connection will be discovered is low, and covered entities should focus on

[20] *Id.* at 23,731.

retaining only the most salient of data following the completion of the final report. Specifically, the mandate that covered entities retain all the "data and information that *may* help identify how a threat actor compromised or potentially compromised an *information system*" is overly broad.[21] Commenters recommend CISA eliminate this line and focus instead on prioritizing the retention of forensic data, as that would be the most relevant to an investigation.

VII. COMMENTERS RECOMMEND CISA MINIMIZE DUPLICATIVE REQUIREMENTS AND PROMOTE HARMONIZATION BETWEEN VARIOUS REPORTING OBLIGATIONS GOVERNING COVERED ENTITIES

CISA has undertaken a series of actions to review the cybersecurity reporting landscape at the federal level, as described in Sections D of the *Proposed Rule*, including serving as a member of the Cyber Incident Reporting Council (CIRC) and engaging with other federal departments.[22] Commenters encourage CISA to harmonize requirements between federal agencies, rather than assigning the task of determining whether reporting obligations can be simplified on the *covered entity*. CISA is obligated, as directed by the White House and in line with the National Cybersecurity Strategy and the recently-issued *National Security Memorandum*,[23] to harmonize its reporting obligations as much as possible with other reporting regulations. In pursuing this objective, Commenters further recommend that CISA leverage the expertise of the Sector Risk Management Agencies and their existing reporting practices when considering harmonization efforts.

A. Requesting Clarification of Harmonization Efforts

[21] *Id.* § 226.13 (emphasis added).

[22] *Id.* at 23,653; *see also id.* at 23,669.

[23] WHITE HOUSE, NATIONAL SECURITY MEMORANDUM ON CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Apr. 30, 2024) ("Departments and agencies shall work to harmonize these efforts to the maximum extent possible through participation in Federal interagency working groups, such as the Cybersecurity Forum for Independent and Executive Branch Regulators…") ("NSM-22"), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience.

There are currently 45 distinct federal *cyber incident* reporting requirements administered by 22 federal agencies.[24] Without harmonization, owners/operators of critical infrastructure cannot safely nor cost-effectively operate their businesses. Commenters are concerned the *Proposed Rule* would require owners/operators to allocate excessive resources to compliance across the federal agencies rather than responding to and recovering from an incident at hand. Covered entities affected by an incident must dedicate significant time and resources to understanding the data related to a covered incident as well as triage the impact of the incident and protect the systems against further intrusions. The onus, as it stands in the *Proposed Rule,* is inappropriately placed on the owners/operators to determine if, and when, there are reporting disagreements between the federal agencies with which they must coordinate. CISA should provide further assistance in streamlining reporting requirements to avoid unnecessary burdens on the *covered entity* so incident response takes precedence to incident reporting to the vast array of government entities. CISA should review the *Proposed Rule* and compare it to the 45 existing regulations to see where it can match existing authorities and reduce duplicated efforts.

Given the definition of a *covered entity* and the definition of a *substantial cyber incident* required to be reported, it is foreseeable that entity operations in other countries or actions taken in other countries might affect U.S. security. Commenters would like clarification on how CISA envisions sharing information with its key intelligence partners, particularly Australia, Canada, New Zealand, and the United Kingdom. For covered entities that have operations in these partner countries, Commenters request further details on how CISA will harmonize the reporting between the countries and ensure that a *covered entity* is both providing and receiving information as

[24] HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT, DEP'T. OF HOMELAND SEC. (Sept. 19, 2023) at 4-5, https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.

necessary. Commenters are curious how CISA plans to account for incidents that occur across the border that could affect U.S. operations as well.

B. Accelerating the Establishment of CIRCIA Agreements to Promote Harmonization

Commenters recommend CISA reassess the contours of the "substantially similar" exception, which permits CISA to identify where reporting requirements for other federal agencies satisfy the mission and objective of the *Proposed Rule*—allowing an entity subject to "substantially similar" rules to report the incident under the existing framework while meeting CIRCIA compliance. Commenters appreciate CISA's commitment to working with the other federal agencies to streamline reporting requirements. Commenters ask that when assessing the possibility of creating CIRCIA Agreements with other federal agencies under 6 U.S.C. § 681b(a)(5)(B), CISA make every effort to establish CIRCIA Agreements so that covered entities can report information as efficiently as possible to the federal government. Commenters also emphasize that CIRCIA Agreements need to be in place and publicly listed, as required under 226.4(a)(5), prior to the rule going into effect. Reporting entities will need clarity on whether their reporting agency has been approved for CIRCIA Agreements prior to a covered incident triggering reporting requirement so that they can deftly comply with their obligations while responding to the incident. The goal of harmonization is to reduce redundancy and confusion while maximizing efficiencies and regulatory outcomes—this can only be accomplished if the *covered entity* has a clear understanding of who they must report to and what they must report. CISA can support covered entities by making their CIRCIA Agreements clear and prioritizing establishing CIRCIA Agreements with the key sector regulators.

The *National Security Memorandum* provides that DHS is to work in "close and continuous coordination" with the SRMAs to ensure a "national unity of effort" to accomplish the goals of the

National Security Memorandum.[25] In line with this goal, Commenters encourage CISA to defer as much as possible to the SRMAs, which are often already collecting relevant information from covered entities. As noted in the *National Security Memorandum*, the National Coordinator is required to review sector-specific guidance and coordinate with the SRMAs to harmonize directives at the national and cross-sector level.[26] Commenters argue that in order to support the mission of the *National Security Memorandum* and to meet harmonization objectives, CISA should put in place CIRCIA Agreements, prior to the rule taking effect, with all of the SRMAs which currently collect or require incident reporting. The burden should rest on the government to properly and securely share information between the different agencies rather than on the *covered entity* such that the owner/operator may focus efforts on responding to the incident.

The "substantially similar" exception provision of the *Proposed Rule* is also an opportunity for CISA to recognize the sensitivity of cybersecurity information. If an entity is already safely and securely submitting this critical information to one agency, it should not be required to open itself up to additional risk by reporting to additional agencies. In addition to these efforts, Commenters encourage CISA to further review its ability to harmonize reporting requirements with existing obligations and to emphasize shared mission objectives between reporting requirements, rather than focusing only on whether the timeframe and content of the reporting are both "substantially similar." Commenters encourage CISA to review how continuous reporting under certain regulatory schemes may, over time, provide the same information that a *covered entity* would provide over the course of providing *supplemental reports* to CISA under the

[25] NSM-22. The National Security Memorandum provides several provisions describing the close coordination efforts required by CISA and the SRMAs, including relying on SRMAs designations to develop recommendations for the President. CISA has historically relied on the expertise of the SRMAs and facilitated in cross-sector coordination with the SRMAs to protect critical infrastructure across the country.

[26] *Id.*

Proposed Rule. CISA acknowledges, and Commenters agree, that not all information requested in the *cyber incident* report may be answered within the first 72 hours. The "substantially similar" exception should acknowledge that other reporting regimes may similarly allow for the *covered entity* to provide the relevant information past the first 72-hour period as well.

Commenters' members also participate in voluntary reporting regimes and adhere to voluntary cybersecurity standards. As noted above, many Commenters' members participate in CRISP, the DOE information sharing framework that necessitates confidentiality. Given Commenters' concerns that submitting information to CRISP might preclude them from submitting information under the *Proposed Rule*, CISA should seek to incorporate information already provided under the CRISP program into the *Proposed Rule* reporting process. This would help alleviate stress on the entities in understanding how they should comply with both agency programs. Additionally, Commenters would emphasize CISA's ability to integrate reporting systems and information it collects under already existing programs housed within the Department. For example, entities participating in the DHS CyberSentry program are already achieving the mission of CIRCIA providing the federal government with visibility into the threat landscape. Commenters would suggest that critical infrastructure owners/operators participating in CyberSentry should provide accommodations to streamline reporting under the *Proposed Rule* given that DHS already has the information being requested through this existing program.

VIII. COMMENTERS RECOMMEND CISA ESTABLISH A MULTI-LAYERED APPROACH TO ENSURING SECURITY THROUGHOUT THE REPORTING PROCESS

Commenters encourage CISA to implement stricter security measures to protect the information provided in the *cyber incident* reports. Commenters appreciate that CISA will employ digital security, including limiting access to the reports and implementing physical and

cybersecurity measures to prevent unauthorized access of information or the exfiltration of information.[27] Commenters strongly encourage CISA to take further steps to ensure the protection of critical information beyond those outlined in the *Proposed Rule*, as outlined below.

First, as previewed in Section IV above, Commenters encourage CISA to refine the amount and type of information to be requested so that it has less information available for the demonstrated potential of unauthorized access. Given the breadth of information CISA will be collecting from the 16 critical infrastructure sectors, CISA will likely continue to be a target of malicious actors. [28] Under the *Proposed Rule*, entities will need to at least provide several high-value pieces of information, including details on the vulnerabilities exploited, the specific products and technologies on which the vulnerabilities were found, and the security controls and protocols the *covered entity* had in place at the time of the incident.[29] Commenters acknowledge that CISA will attempt to reduce the amount of personal information it collects to the information it deems necessary for understanding the reports.[30] However, Commenters are concerned that the structure of the *Proposed Rule* will result in covered entities over reporting information relating to a covered *cyber incident* in order to assure full compliance with the reporting rule. This would lead to an overproduction of sensitive information that further endangers CISA as a cyber target.

To address these security concerns, Commenters recommend that CISA incorporate a multi-layered approach to data security that would address security before, during, and after the

---

[27] *Proposed Rule* at 23,741.

[28] Consider the recent news that CISA identified a threat actor's exploitation of the Infrastructure Protection Gateway and Chemical Security Assessment Tool. *See* Matt Kapko, *CISA Attacked in Ivanti Vulnerabilities Exploit Rush*, CYBERSECURITYDIVE (Mar. 11, 2024), https://www.cybersecuritydive.com/news/cisa-attacked-ivanti-cve-exploits/709893/.

[29] 6 U.S.C. § 681b(c)(4)(B) ("a description of the vulnerabilities exploited, security defenses in place, as well as the tactics, techniques and procedures used to perpetrate the covered cyber incident").

[30] *Proposed Rule* at 23,740 ("Instructions for Personal Information").

reporting process. In carrying out security protocols to protect the information submitted to the agency, Commenters ask that CISA provide complete visibility for covered entities into how the data will be managed and secured throughout its lifecycle.

Commenters further recommend that CISA provide an alternative reporting process for the most critically sensitive information that would provide enhanced security protocols to prevent the data from being exploited. Commenters look forward to partnering with CISA to determine how they can best secure the information they provide so that CISA can in turn help secure the systems they operate.

IX. CONCLUSION

Commenters and their members are committed to advancing national security by safeguarding critical infrastructure from increasingly sophisticated attacks. We applaud CISA's efforts in focusing on incidents that actually jeopardize operations. While seeking to facilitate an effective partnership with industry and implement CIRCIA, CISA must ensure that reporting requirements complement rather than jeopardize operator responses to cyber incidents. By requiring 72-hour reporting of only the most pertinent information, CISA would free industry partners to prioritize incident response and mitigation. CISA requirements should also promote the best use of operators' limited resources. To this end, Commenters recommend CISA clarify the type of information to be retained and the retention timeline following an incident. Harmonizing requirements from various government agencies and ensuring that reporting requirements affect only the entity in the supply chain most capable of providing an informative report will minimize redundancy and waste in the aftermath of a significant incident. Finally, all strong partnerships rely on trust, and sensitive information entrusted to CISA must be protected. The aggregation of sensitive information presents an enticing target for malicious actors seeking to exploit

vulnerabilities. Commenters appreciate the opportunity to inform development of this important rulemaking and trust that adoption of the recommendations will properly serve national security interests and the reporters in the wake of an incident.

Respectfully submitted,

July 3, 2024

Kimberly Denbow
Vice President, Security and Operations
American Gas Association

Suzanne Lemieux
Director, Security and Emergency Management
American Petroleum Institute

Maggie O'Connell
Director of Security, Reliability, and Resilience
Interstate Natural Gas Association of America

Stuart Saulters
Vice President of Government Relations
American Public Gas Association