American
Fuel & Petrochemical
Manufacturers

1800 M Street, NW
Suite 900 North
Washington, DC
20036

202.457.0480 office
202.457.0486 fax
afpm.org

July 3, 2024

Mr. Klessman
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
2707 Martin Luther King Jr. Ave. SE.,
Washington, DC 20528

Attention: Docket ID No, CISA-2022-0010
Submitted to the Federal eRulemaking Portal (www.regulations.gov)

Re: DHS/CISA Notice of Proposed Rulemaking titled "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements"

Dear Mr. Klessman,

The American Fuel & Petrochemical Manufacturers (AFPM) is pleased to submit these comments on the proposed Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements rule, 89 Fed. Reg. 23644 (April 4, 2024). AFPM supports one set of federal regulations requiring a one-time cyber incident report to a single federal agency; however, we encourage the Cybersecurity and Infrastructure Security Agency (CISA) to better describe the purpose of the reporting rule, clarify certain terms and definitions within the proposal, develop a risk-based approach throughout the rule, and focus its efforts on cybersecurity incidents intentionally targeting critical infrastructure that have significant national security implications. Harmonization is crucial to implementing a simple and effective reporting program. Therefore, CISA should finalize agreements with other agencies before the effective date of the CIRCIA rule.

I. Introduction

AFPM is a national trade association representing nearly all U.S. refining and petrochemical manufacturing capacity. AFPM members support more than three million quality jobs, contribute to our nation's economic and national security, and enable the production of thousands of vital products used by families and businesses throughout the United States.

Due to the vital importance of the products we produce, AFPM and its members have been involved in the development of cybersecurity policy and regulations since the inception of U.S. Coast Guard's (USCG) Maritime Transportation Security Act (MTSA_ and the Chemical

Facility Antiterrorism Standards (CFATS) regulations. AFPM members are subject to a myriad of cybersecurity and physical security regulations such as CFATS, the MTSA, the Transportation Security Administration's Pipeline Cybersecurity Security Directives (TSA SDs), and the Securities and Exchange Commission's (SEC) Cyber Incident Reporting rule.

II. AFPM Supports a One Time Obligation to Report Cyber Security Incidents to a Single Government Agency

In general, in the event of a significant cybersecurity incident impacting a covered entity, AFPM supports the submission of a single report to one agency within a reasonable time. There are currently 45 distinct federal cyber incident reporting requirements administered by 22 federal agencies. Without some type of harmonization effort and efficient reporting structure, owners and operators of critical infrastructure cannot effectively and efficiently protect their businesses and coordinate responses with CISA. For example, multiple federal agencies, such as the USCG proposed Cybersecurity in the Marine Transportation System (Docket No. USCG–2022–0802), which proposes cyber incident reporting obligations. To ensure efficiency and avoid confusion, we propose that one federal agency be responsible for receiving reports and notifying other federal agencies as appropriate. We recommend that CISA serve as the recipient of all reports. CISA would in turn inform and involve other federal agencies such as the TSA, Coast Guard, or others as appropriate. This would allow both regulatory agencies and the covered entity to focus on incident response. CISA should resolve regulatory harmonization as required by the National Cybersecurity Strategy before the effective date of any of the various cybersecurity reporting rules to ensure smooth implementation.

III. The Definitions Impacting the Applicability of this Rule Should be Narrowed

1. Covered Entity

The term covered entity is a key term in the proposed regulation, as it is the operative term used to describe the regulated parties that would be subject to the final regulations of this proposal. Section 226.1 describes the applicability of the rule to certain entities within critical infrastructure sectors. AFPM understands CISA's desire to include important entities from each of the 16 Critical Infrastructure Sectors. Most relevant to AFPM members would be the chemical, energy (refining and pipelines), and transportation (MTSA) sectors. CISA's expectation that more than 300,00 entities would be covered under the proposed rule and the estimated potential for a high number of annual reports. CISA estimates that 316,244 entities would be considered covered entities under the proposed rule.[1] When combined with the breadth of the proposed substantial (covered) cyber incident definition, CISA is likely to receive far more

[1] https://www.federalregister.gov/d/2024-06526/p-1367; https://www.federalregister.gov/d/2024-06526/p-1370

than the 15,812 annual incident reports it anticipates receiving.[2] AFPM is concerned that CISA and other agencies lack the personnel to manage the expected deluge of annual reports, however, CISA's proposed approach and scope of the reporting requirements appears to be so broadly applicable that it is questionable whether CISA has the resources to properly respond to a deluge of information. The reportable cyber incidents must be risk based or it will result in CISA potentially covering hundreds of thousands of entities and leaving inadequate federal staff to manage and respond to the expected reports. Reporting of cyber incidents would come from facilities that, while technically falling within a Critical Infrastructure Sector, may not be in fact "critical" from a national security perspective.

Instead, CISA should take a risk-based approach. Implementing a risk-based reporting rule will allow CISA to more effectively deploy its resources by narrowing the scope of the reporting requirements, refining definitions of a ***covered entity,*** and a ***covered cyber incident*** order to enable more effective reporting. AFPM strongly recommends CISA:

- Focus the scope of CIRCIA reporting so that it only applies to a subset of critical infrastructure entities so that it is risk based. For example, this could be done by applying the reporting requirement only to past high ranked CFATS sites, TSA SD sites and USCG MTSA sites with certain dangerous chemicals onsite (CDCs).

- Refine the definitions of a covered cyber incident/substantial cyber incident to just the top three criteria to prevent overreporting.

- Emphasize the importance of harmonization by mandating timelines for the finalization of interagency information sharing agreements, which should help minimize burdens on the cybersecurity workforce.

- Emphasize the quality of information reported, not the quantity of information reported.

CISA argues that it is appropriate to define entities within a critical infrastructure sector consistently with sector-specific plan (SSP) profiles that were "developed through a collaborative public-private partnership, as these sector profiles reflect a mutual understanding of what types of entities are in a critical infrastructure sector."[3]

[2] https://www.federalregister.gov/d/2024-06526/p-1389

[3] https://www.federalregister.gov/d/2024-06526/p-631

CISA estimates that 316,244 entities would be considered covered entities under the proposed rule.[4] AFPM recommends that CISA should adopt a more targeted, risk-based approach to covering entities. The definition of a covered entity should be tightly construed to include only those entities whose operations and functions pose an immediate, high-level risk with severe and adverse consequences to national security, economic security, or public health and safety. America's critical infrastructure needs this program to be successful, however by this definition, AFPM fears that requiring too many entities reporting to CISA will cause a dangerous backlog for CISA to assist in incident response and will only obscure possible troubling trends that CISA otherwise could identify and lead to larger and more costly cyber incidents.

2. Trade Association Applicability

On page 23676 of the proposal, it states that "CISA interprets the word "entity" to be a broad term, generally including any person, partnership, business, **association,** corporation, or other organization (whether for-profit, not-for-profit, nonprofit, or government) regardless of governance model that has legal standing and is uniquely identifiable from other entities.*"*

Building off their definition of "entity," the NPRM notes that Critical Infrastructure Sector Specific Plans are developed by "some entities that do not own or operate systems or assets that meet the definition of critical infrastructure in Presidential Policy Directive (PPD)-21 but are active participants in critical infrastructure sectors and communities, are considered 'in a critical infrastructure sector.'" Furthermore, the proposal states that "CISA proposes to include an equivalently wide variety of types of entities within the scope of the CIRCIA regulatory description of 'covered entity' to reflect the same diversity of entities that are in a critical infrastructure sector within the context of PPD-21, the National Infrastructure Protection Plan (NIPP), and each sector's SSP."

This suggests that if a trade association participates in a sector's coordinating council (SCC), they may be considered a covered entity. This is illogical and unlawful since trade associations like AFPM are not critical infrastructure and are not defined as critical infrastructure under the statute. AFPM is a member of both the Oil and Natural Gas (ONG) and Chemical Sector Councils, but it cannot be considered a covered entity under the statute. Because they do not operate infrastructure, they cannot be critical infrastructure. Moreover, this may discourage trade association participation in these programs, which will undermine cybersecurity. CISA should clarify that trade associations are not covered entities.

3. The Final Rule Should Revise Provisions to Report Substantial Cyber Incidents that Jeopardize the Availability of Information or Information Systems

[4] https://www.federalregister.gov/d/2024-06526/p-1367; https://www.federalregister.gov/d/2024-06526/p-1370.

CISA properly focuses the covered cyber incidents on only those that rise to the level of "substantial" and "serious" as set forth under paragraphs (1) and (2) of the definition of "substantial cyber incident" (seen on page 6). Likewise, the focus on actual "disruption" as a trigger to reporting in paragraph (3) is appropriate. However, paragraph (4) concerning any "unauthorized access" to an entity's information systems or networks is so broad as to ensure a deluge of marginal reports of little import to CISA's mission. For example, a single company may experience thousands of low-level intrusions, password-guessing, etc. daily. To require a report of every instance of an invalid password is unworkable and will result in thousands of meaningless reports to CISA.

As stressed in the statute, CISA should seek information on cyber incidents that jeopardize information systems and "do not include any occurrence that imminently, but not actually, jeopardizes" information systems.[5] For this definition, Section 226.1 of the Proposed Rule provides that a substantial cyber incident is one that leads to any of the following:

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

4. Unauthorized access to a covered entity's information system or network, or any nonpublic information contain therein

These impacts should correspond with events that *actually jeopardize* an entity's systems, as required by statute.

In meeting the statutory objective, CISA should raise the threshold for substantial cyber incidents that must be reported. For example, the definition of "substantial cyber incidents" should not include a member's website operations being impacted because such an event, while inconvenient for a site, does not *actually jeopardize* the availability of information or the information system itself. This type of incident would not disrupt production operations for an AFPM member and, as such, should not need to be reported as it is not considered jeopardizing. The final rule should confirm that the definition of "substantial cyber incident" excludes information that does not jeopardize the availability of information or the information system to avoid the overreporting. Absent further clarification, the operator would spend significant time reporting incidents that on a risk-scale would have minimal significance and would distract from securing the systems.

[5] PUB. L. NO. 117-103.

Therefore, CISA should 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." CISA should take a risk-based approach that focuses on the mission of knowing/responding to breaches that impact national security. We offer the following revisions:

1. The definition of "substantial cyber incident" (section 226.1) should be revised as follows.

Substantial cyber incident means a cyber incident that affects the ability to operate the critical infrastructure asset as defined by the sector-based criteria established in 226.2, which leads to any of the following

1) A substantial loss of confidentiality, integrity or availability of a covered entity's information system, ~~or~~ network, cloud service provider, or supply chain information that provides those services;
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;
~~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 provide, managed service provider, or other third-party data hosting provider;~~
~~ii) Supply chain compromise~~

A substantial incident should be narrowly tailored to impacted entities which fall under the critical infrastructure asset criteria. The proposed language is intended to clarify what is meant by the term "substantial" because the proposed definition does not explain whether "substantial" is tied to impacts on the individual company, the nature of the threat in absolute terms, or relative to the size of the company. The proposed definition also reasonably limits the scope of reportable incidents. Similarly, we propose deleting the separate reference to supply chain access as it is too broad of an item to be classified under substantial cyber incident.

AFPM suggests limiting the requirement to report supply chain information that results in a "substantial loss" "of confidentiality, integrity, or availability of a covered entity's information system or network." To assist in considering this change, find below two examples involving a cyber incident within the supply chain that would not result in a "substantial loss":

Example 1: Company A uses a 3rd party provider as a broker for shipping products (e.g., arranging shipments, finding lowest cost). The broker company has a cyber security incident which leads to some data loss, but this does not have a material impact on Company A. Information leaked includes company name, product name, customer name, but not quantity / pricing.

Example 2: Company A uses a 3rd party provider to support the company with an activity. The 3rd party provider suffered a ransomware incident which caused an outage of 3rd party environment for a week. During that week, the Business Continuity processes are implemented by the 3rd party which results in no impact for Company A. (Product is still shipped on time, etc.)

Should CISA not accept these proposed amendments, the agency should consider using Australia's definition of cybersecurity incident as defined in The Security of Critical Infrastructure Act 2018 (the SOCI Act). The SOCI Act provides for mandatory cyber incident reporting for critical infrastructure assets. Critical infrastructure owners and operators are required to report on incidents that apply to incidents that have "significant impacts" on covered assets and incorporate the specific qualifiers for reporting [6:]

> A cyber security incident is one or more acts, events or circumstances involving: - unauthorized access to or modification of computer data or computer program, or - unauthorized impairment of electronic communications to or from a computer, or - unauthorized impairment of the availability, reliability, security or operation of computer data, a computer program or a computer.

To further ensure reporting of substantial cyber incidents, CISA should collaborate with stakeholders to specify what quantifiable metrics should be. Otherwise, CISA will likely be inundated with suspicious activity reports such that the purpose for the reporting rule will be swallowed by the volume of marginal reports. Focus should be given to CISA's role as an information hub geared toward rapid dissemination of information to assist with the response, rather than simply compiling data and making monthly reports. CISA has a more important role to play and should not lose sight of the mission.

IV. Ransom Payment Should Not Be Reported Under this Rule

CISA should not require entities to report ransom payments to CISA. Deciding on whether to pay during a ransomware incident is a business decision that will vary with each entity that may not always affect the cybersecurity of a site. Ransom payments should not transform an otherwise reportable incident into a reportable one. CISA has not adequately explained why this must be reported within 24 hours, as ransomware payment is a business decision and reporting must be considered very thoughtfully. CISA should focus only on those incidents that would actually jeopardize operations of critical infrastructure sites that would impact national security—payment of ransomware would not affect a site's operation or national security.

V. Substantially Similar Reporting Exception

[6] cyber-security-incident-reporting.pdf (cisc.gov.au):

The substantially similar exception provision of the CIRCIA rule is a great opportunity for CISA to recognize the sensitivity of cybersecurity information. The substantially similar exception of the proposed rule provides that an entity is safely and securely submitting this critical information to one agency, and it should not be required to open itself up to additional risk by duplicative reporting to other agencies. AFPM is encouraged that CISA acknowledges not all information requested in the cyber incident report may be answered within the first 72 hours, and the "substantially similar" exception should acknowledge that other reporting regimes may also allow for the covered entity to provide the relevant information past the first 72-hour period. It is imperative that CISA include in the final rule a list of agencies with which they have signed agreements. Additionally, it is important that CISA does not promulgate unnecessary requirements that cause its reporting requirements to diverge from other requirements, with the result that companies are precluded from taking advantage of this exception.

VI. Covered Entities Should Not Be Required to Report Supply Chain Compromises as They Would Not Have Access to this Information

CISA should reassess the assignment of responsibility for incident reporting along the supply chain and should not require critical infrastructure owners and operators to report cyber incidents along their supply chain. AFPM agrees with CISA that reporting requirements should consider cascading impacts along the supply chain; however, the responsibility of reporting a cyber incident on a supplier should be placed primarily on the entity who suffered the cyber incident. AFPM members do not possess this information. Specifically, AFPM members will not be able to provide several elements required under Section 226.8, including the below information:

- Descriptions of 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 of 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.

Covered entities are customers and may not be notified by their supplier of a cyber incident. Therefore, they should not be held responsible for reporting a supplier's breach. However, if CISA pursues supply chain disclosure it should only be if it significantly impacts the company's own security or there is no benefit to disclosure and it's just an arbitrary paperwork burden. The final regulations should encourage and even incentivize courtesy notifications.

CISA should reevaluate how this applies to major suppliers of actual critical infrastructure (e.g., power, water, industrial gases, refiners, and petrochemicals). Requiring a supplier's customers to report under this provision will be largely ineffective as the customers will not have the same access to critical information relating to the incident as the affected entity.

In conclusion, AFPM members do not have access to information regarding the nature of the cyber incident and the security protocols used by the affected vendor or supplier. The reports submitted by the operator in this scenario would be mostly blank, making supply chain reporting an ineffective use of operator's resources that would not advance the objective of CIRCIA and will further inundate CISA with unhelpful reports.

VII. AFPM Supports Reporting to One Government Entity as AFPM Members Are in Multiple Sectors

As previously noted, AFPM members represent both the refining and petrochemical industry and are in the chemical, energy (refining and pipelines), and transportation (MTSA) sector designations of this proposed rule. As members of multiple sectors, AFPM members

could be subject to multiple cyber incident reporting rules (TSA SDs, USCG cyber security rule and CFATS (when it was authorized)), many members could be subject to three separate cyber security rules that contained cyber incident reporting. As discussed throughout these comments, AFPM supports developing a program where a critical infrastructure entity would only have to report to one government entity. Allowing a one stop reporting would lessen some duplicative burden on industry, allow CISA to review the reported cyber incident immediately and coordinate a response (if needed) with other applicable agencies (USCG, TSA, etc.).

1. Chemical

According to the proposed rule, if the CFATS program is not reauthorized by the time of final rule, then sites subject to the Risk Management Plan (RMP) rule will need to be notified that they are subject to this rule. A vast majority of AFPM member sites are subject to the RMP rule. However, the RMP rule applicability is not risk based and CISA would be receiving cyber incident reports from potentially far more sites than if limited to CFATS sites or sites previously subject to CFATS regulations. Specifically, CISA would have to revise the current proposals regulatory impact and cost benefit analysis before publishing a final rule subjecting RMP sites to this rule.

2. Transportation Systems

Many AFPM members have pipelines that are subject to the TSA's Pipeline Security Directives. CISA needs to recognize that several provisions that are duplicative if not the same in this proposed rule reflect the same principles incorporated by TSA in the 2021 Security Directives 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 feedback from the industry and changes in the cyberthreat landscape.[7] 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. AFPM members subject to the Security Directives are actively securing their networks to comply with these requirements and will continue to share information with the federal government through these existing channels and collaborate with the federal government. The Security Directives will soon become part of large cybersecurity regulation for the surface transportation sector, and we ask CISA to encourage these varied agencies to develop agreements with CISA to allow critical infrastructure subject to their cyber security regulations to report once to CISA after a cyber incident.

3. MTSA Sites

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

At least half of AFPM member sites (e.g., terminals, refineries, and petrochemical) are subject to the MTSA regulations and would be subject to the eventual USCG final rule, "Cybersecurity in the Marine Transportation System." In the Cybersecurity in the Marine Transportation System proposed rule the USCG AFPM commented on the proposed rule and supported the USCG option of exploring with CISA reporting once to CISA under the CIRCIA rule. AFPM encourages CISA and the USCG to establish an agreement that would allow MTSA sites to report cyber incidents to CISA.

VII. The Content of Initial Incident Reports Should Reflect Available Information

CISA should focus on its mission to ensure US critical infrastructure is resilient and remains in operation. If regulatory requirements are complicated and burdensome, the covered entity resources will be diverted to fulfilling reporting obligations rather than addressing the incident. Reporting needs to be simple, fast, and effective. CISA should reduce and refine the amount of information required for the initial incident reports because more detailed information may not be available within 72 hours. Covered entities will need more to understand the nature of the incident and determine whether the impact fits the definition of Section 226.1 of a substantial cyber incident. Our members report that companies will not have all the information required for the report until as long as day 7 after an incident. If the final rule does not allow for more time (i.e., 96 hours), a supplemental report will be necessary.

Focusing on the initial report will accomplish the goal of ensuring CISA has notice of an incident while not pulling company resources away from recovery. Supplemental reporting can provide further detail. The following information that should be requested within the first 72 hours following an incident:

- The threat level and risk of the incident,
- The estimated timeline of the incident – specifically, when the attack is believed to have begun, and
- The indicators of compromise as seen on their system.

CISA should make the content, form, and manner of reporting more practical and offers the following comments for consideration:

- Reconsider the data and records preservation requirements so that entities' resources principally go to cybersecurity measures, not recordkeeping. The proposed rule would require any covered entity that submits a report under CIRCIA to preserve data and[i] records (D&R). The NPRM would require a covered entity that submits a CIRCIA report to begin preserving D&Rs for 2 years from the date in which an entity (1) establishes a reasonable belief that a covered cyber incident occurs or (2) makes a

ransom payment. The NPRM states that the 2-year retention period would restart at the time of submission of each supplemental report.[8] AFPM recommends reducing the D&Rs preservation requirement to 1 year. AFPM also recommend revising § 226.13 to enable a covered entity to determine the D&Rs it preserves related a covered cyber incident or a ransom payment. By limiting the scope of the requirement to relevant D&Rs, it would provide covered entities with much-needed clarity and ensure that resource-constrained entities are not diverting resources from mitigation and remediation efforts to preserving D&Rs that would not meaningfully add value to investigative efforts.

- Safeguard private-sector information entrusted to CISA that is of paramount concern to critical infrastructure owner and operators particularly after the recent breach of the CFATS CSAT portal.

- Establish *ex parte* communications for the CIRCIA rulemaking.

- Reassess the approach to enforcement regarding CISA issuing subpoenas to a business for information.

Finally, CISA should treat reporting as a means to bidirectional sharing and operational collaboration. Cyber incident data reported to CISA needs to be promptly aggregated, anonymized, analyzed, and shared with industry to foster the reduction and/or prevention of future cyber incidents. In recent years, the threat and information sharing from CISA, and other government agencies has increased, and the quality has definitely improved. The CIRCIA rulemaking is a prime opportunity to build on improved bidirectional information sharing and operational collaboration between CISA and private sectors.

VIII. Supplemental Reporting

The supplemental report should only be required at the conclusion of an incident or when the new information is considered material and not when "any" new information has been received. However, should the language remain as is, covered entities could make upwards of three supplemental reports to CISA while in the midst of incident response, which would detract critical resources from response. AFPM proposes the requirement for submission be changed from "promptly" to "without undue delay." This allows covered entities to report in a timely manner without the risk of penalization while in the midst of an incident response. This also aligns with CISA's interpretation in the preamble (p. 23726). Should CISA not accept these proposed changes, then requiring supplemental reports every 72 hours (or 3 business days) from the time an initial report is submitted may be sufficient. This frequency would prevent entities from reporting daily minor information that may be required in the supplemental report and would establish a regular cadence for reporting.

[8] https://www.federalregister.gov/d/2024-06526/p-1246

IX. Ransom Ware Incident Reporting Time

As described in Section IV, AFPM reiterates that CISA not make it mandatory that ransom payments be reported to CISA. This is a business decision that will vary with each entity that may not always affect the cyber security of a site. AFPM questions the logic behind reporting that to CISA within 24 hours, as ransomware payment is a business decision and reporting must be considered very thoughtfully.

X. Enforcement

1. The Proposed Term "Authorized Purpose" Should Only Be Used to Prosecute Nation-State Actors and Criminal Organizations

CISA proposes to create a newly "authorized purpose" in the CIRCIA rule allowing information to be used for "preventing, investigating, disrupting, or prosecuting an offense" arising out of "events" required to be reported to CISA (e.g., in a CIRCIA Report or a response to a Request for Information). CISA says that this information would be used by federal law enforcement agencies to "investigate, identify, capture, and prosecute perpetrators of cybercrime." AFPM strongly supports the government's efforts to degrade or disrupt the cyber operations of foreign powers or their surrogates and international criminal gangs. CIRCIA's confidentiality safeguards, liability protections, and authorized use restrictions should prevent the government using reported information against industry in legal actions. As written, the proposed rule could undermine these protections and discourage private entities from sharing information with CISA other than what is absolutely required—an outcome that would undermine the very objective of CIRCIA.

2. Clarify § 226.20 Regarding Penalties for False Statements or Representations

To avoid regulatory misinterpretations, the CIRCIA rule should incorporate language from CISA's preamble clarifying that a covered entity is not liable for false statements or representations where it reports information that it reasonably believes to be true at the time of submission, but later learns was not correct and submits a Supplemental Report reflecting the new information in order to inform CISA further information on the cyber incident that could help CISA possibly identify tactics and techniques of those conducting cyber security incidents. CISA should not use § 226.20 to pursue claims against covered entities.

AFPM strongly supports the reporting of cyber incidents to a single federal agency, specifically, to CISA. However, as proposed, this may result in an overreporting of immaterial information which may impede CISA's ability to share critical information efficiently to the affected critical infrastructure. The single reporting entity program should focus on vital

information related to impact criteria, ransomware, supply chain compromise—to ensure that CISA is not inundated with reports regarding insignificant risks. CISA should minimize duplicative cybersecurity regulatory requirements and promote harmonization between the various reporting obligations governing covered entities, including by addressing regulatory harmonization as outlined in the National Cybersecurity Strategy. This would allow the covered entity to focus on incident response rather than report to multiple agencies.

America's critical infrastructure depends on CISA focusing on its mission and to quickly disseminate *relevant* information, help coordinate an appropriate response, share key intelligence with industry, and collaborate with stakeholders to secure the homeland. Industry and CISA both need to share the same vision, and the rule must be effective and workable by both CISA and America's critical infrastructure. The threat is serious and the more focused, determined, and clear the rule, the more effective we will all be against very real adversaries.

AFPM and its members look forward to continuing our collaborative work with CISA on this important rulemaking. If you need further information or have any questions, please contact Jeff Gunnulfsen at jgunnulfsen@afpm.org or at 202-844-5483.

Sincerely,

Jeff Gunnulfsen
Senior Director-Security & Risk Management Issues
AFPM