July 2, 2024

Cybersecurity and Infrastructure Security Agency
US Department of Homeland Security
245 Murray Lane, Stop 0380
Washington, DC 20528-0380

RE: CISA Notice of Proposed Rulemaking, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," CISA-2022-0010, 89 Federal Register 23644 (April 4, 2024)

The Information Technology-Sector Coordinating Council (IT-SCC) and the Information Technology-Information Sharing and Analysis Center (IT-ISAC) greatly value the opportunity to provide a joint response to the proposed CIRCIA regulations published on April 4, 2024. While we appreciate CISA's thoughtful approach, we nonetheless see opportunities for refining and improving the proposed regulations with the goals of ensuring they are properly scoped, clearly understood, and easy to implement without overwhelming CISA's ability to ingest and analyze the submitted information so that it can produce valuable and actionable threat intelligence to industry. Current aspects of the proposed regulations are relatively broad, costly, and unclear. We provide more details on specific areas of concern in our comments below.

However, we first would like to emphasize the importance of getting these regulations right. The purpose of the authorizing legislation was not to pull as much information as possible into CISA. Rather, the goal was to provide CISA information to understand, prevent, identify, and respond to threats—including providing actionable threat intelligence back to the critical infrastructure owners and operators. At times, it appears this last purpose—the sharing of threat intelligence beyond the federal enterprise—has been pushed into the background and deprioritized. Additionally, CIRCIA's direction to DHS to establish the Cyber Incident Reporting Council, with a mandate to harmonize Federal incident reporting requirements, including those established by CIRCIA, indicate Congress's intent for CIRCIA reporting to contribute to overall efforts to harmonize federal cyber incident reporting requirements.

Portions of the regulations entail a high cost of compliance. Hundreds of thousands of small entities (the proposed regulations estimate that 310,000 of the 316,000 impacted entities are small entities) will bear the disproportionate impact of the proposed regulation. Ensuring compliance to this level likely will require diverting resources from security defenses. Compared to instituting defensive security measures, compliance is more difficult and more expensive for these entities, and the value they will receive in return is uncertain at best.

To better understand and address the potential consequences of these far-reaching regulations, it is important that CISA establish a process similar to that followed by the FCC: allowing additional meetings with impacted communities, especially Sector Coordinating Councils and ISACs, and additional filings after the comment period ends. The regulations' vast economic impact (which we think are underestimated), the need to ensure that the "covered cyber incidents" are scoped in a

manner that provides value to industry and government, and the desire to preserve CISA's role as a trusted partner justify continued dialogue with stakeholders after the initial public comment period expires.

With that, we are pleased to provide comments on specific aspects of the proposed regulations.

1. Definition of Covered Entity:

CISA provides four general criteria to determine a "Covered Entity" within the IT Sector. The first of these is "any entity that knowingly provides IT hardware, software, systems, or services to the Federal government." Regarding the word "Services," it is unclear as to whether this means a company that provides any service to the government, or whether this is limited to IT Services provided to the government. Based on the context, we believe the intent is to limit it to "IT Services" and request that the proposed regulations be clarified as such— "any entity that knowingly provides IT hardware, software, IT systems, or IT services to the Federal government." Additionally, CISA should modify the second and third criteria within the IT Sector to align with CIRCIA's statutory factors for covered entities. Specifically, CISA should narrow the second criteria (related to "critical software") and the third criteria (related to operational hardware and software) to apply only to entities that knowingly provide or support the critical software or OT hardware or software components to another entity within the nation's critical infrastructure.

Similarly, CISA proposes that "any entity that is an original equipment manufacturer (OEM), vendor, or integrator of OT hardware or software components" is a "covered entity ". We believe the meaning of this section is that "software components" refers to companies that provide OT software rather than companies that provide any software. Clarification is needed

2. Definition of Covered Cyber Incident

Defining a Covered Cyber Incident to be a "substantial cyber incident" helps narrow the scope of reporting to actual incidents that have occurred. A "substantial cyber incident" is defined as follows:

> *A cyber incident that leads to any of the following (a) a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network; (b) a serious impact on the safety and resiliency of a covered entity's operational systems and processes; (c) a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or (d) 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. CISA is further proposing that a substantial cyber incident resulting in one of the listed impacts include any cyber incident regardless of cause, including, but not limited to, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.*

We very much appreciate CISA's attempts to refine the scale of the reporting requirements, but we suggest that the definition does not account for the criticality of the network or system to the covered entity or the severity of the disruption.

For example, we recommend criteria (a) should clarify that the "system or network" be critical to the covered entities operations. Criteria (b) should limit the requirement to "systems and processes that are critical to its operations".

Criteria (c)— "a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services" —should also be further refined. Not all business "disruptions" are critical events with meaningful impacts. An incident that could cause a limited disruption of operations may not have any meaningful impact on the business. As such, we suggest that the criteria be changed to require *severe* disruption in the covered entity's ability to engage in its critical operations.

We have similar feedback related to criteria (d)—that covered entities report compromises through supply chain partners, MSPs, or cloud providers. It is not clear why a supply chain attack, on its own, is a substantial cyber incident even if it does not result in any impact. The fact that a covered entity's third party experienced a substantial cyber incident does not mean that the covered entity itself experienced a substantial cyber incident. Moreover, the fact that a third party experienced a "covered cyber incident" should trigger a reporting requirement for a covered entity *only* if that incident caused a substantial cyber incident on the customer covered entity.

The definition of a supply chain compromise is unclear: "*Supply chain compromise means a cyber incident within the supply chain of an information system that an adversary can leverage, or does leverage, to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle."*

The use of the words "can leverage" seems to imply that a vulnerability, rather than an actual incident, constitutes a reporting obligation. This section can be interpreted to say that a covered entity must report vulnerabilities that are contained on or within a third-party provider. This is not appropriate because in many cases, the covered entity will have no way to determine whether their third-party provider has a vulnerability. A covered entity cannot be expected to report a vulnerability of a third party. However, even if it is clarified that entities need to only report vulnerabilities they know about from a third party, this will result in a lot of repetitive reporting on the same vulnerability, even if that vulnerability produces no impacts.

Relatedly, CISA also has defined a "covered entity" within the IT sector as "any entity that has developed and continues to sell, license, or maintain any software that meets the definition of 'critical software' established by NIST pursuant to Executive Order 14028." We certainly understand the importance of critical software, but it is less clear why these companies are being asked to report cyber incidents that do not impact the integrity of the critical software.

For example, under the proposed regulations, an attack that disrupts the email systems of a company that produces critical software is a reportable incident, even if there is no risk to the critical software itself. If the interest is in the security of the critical software, we suggest that a reporting requirement be confined to substantial cyber incidents that impact the security, confidentiality, and integrity of the critical software provided by the covered entity.

When describing the reporting requirements for IT Sector "Covered Entities," the regulations state:

> *Note, however, while CISA is proposing to use the provision of software, hardware, systems, or services to the Federal government as a criterion for determining who must report, reporting for those entities that meet this sector-based covered entity criteria is not limited to incidents impacting the products or services they provide to the U.S. Government. Rather, an entity that meets this sector-based criteria must report any covered cyber incident it experiences regardless of whether it impacts any of their Federal customers or the specific products or services used by their Federal customers.*

This seems to state that IT Sector companies must report substantial cyber incidents experienced through "the products" of the covered entity. This is confusing, as a substantial cyber incident is

defined as impacting the operations of the covered entity. An issue in a product may not be disruptive to that product manufacturer's business operations.

Therefore, we are seeking clarity as to what constitutes a reportable event in terms of product security.

- Must a company that makes an IT product report all known exploits of a vulnerability, even if the exploited vulnerability is not known to have caused a substantial cyber incident within any customer?
- Must a company report as a substantial cyber incident that an exploit of a vulnerability was used to cause a substantial cyber incident for a customer?
- What if the substantial cyber incident was caused by a customer not deploying a fix that was available to it?
- What if the incident was caused by a customer turning off or reducing the deployed default enhanced security setting (the vendor ships the product with MFA enabled, but it is turned off by the customer)?

Relatedly, the proposed regulations include the following definition of "cyber incident": '*an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or actually jeopardizes, without lawful authority, an information system*."

As a general matter, we do not believe that a vulnerability in a product or service is a "covered cyber incident" for either the manufacturer of the product or its customer. Not every vulnerability results in an exploit. According to Intel 47, the National Vulnerability Database reports that in 2023, it recorded 28,831 vulnerabilities. Of these, only 187 vulnerabilities were added to the Known Exploited Vulnerabilities list. It is not plausible, efficient, or fiscally responsible to require entities to report on every vulnerability in their product line or in their enterprise.

The rest of the regulations focus on cyber incidents that actually occur, but this definition refers to incidents as jeopardizing. What does "actually jeopardize" mean, and how is that determined? Merriam Webster defines "jeopardize" as: "to expose to danger or risk." A discovery of a vulnerability on a system can increase risk to a system or "jeopardize" data hosted on it. However, having a vulnerability on a system does not mean that the system or data was actually accessed.

Section 2240 of the law clarifies that a cyber incident ''does not include an occurrence that imminently, but not actually, jeopardizes— (i) information on information systems; or (ii) information systems." In other words, there needs to be an actual impact, not the just risk or exposure.

We support defining a covered incident as having actual impacts, but find it confusing that the definition of "cyber incident" does not include an impact.

Finally, we are seeking clarity as to whether a covered cyber incident relates to only systems or impacts in the U.S., or if covered entities will be required to report on substantial cyber incidents regardless of whether they take place on, or impact, U.S.-based networks. We suggest that the requirement be focused on U.S. networks or, in terms of supply chain compromises, if the incident impacts covered entities in the U.S.

3. Reporting Timeline

As currently proposed, the timeline for reporting an incident is 72 hours from when a covered entity "reasonably believes" that it has experienced a substantial cyber incident. We request that CISA amend this to 72 hours from when a Covered Entity "confirms" or "determines" that it has experienced a substantial cyber incident. This provides the Covered Entity clarity on what the reporting requirements are, thereby reducing potential liabilities and misunderstandings. Further, it helps companies balance the need to investigate an incident with the requirement to report an incident. This is especially important for small enterprises who lack substantial internal response teams; forcing them to pivot from incident response and management to reporting prior to confirming the enterprise is a victim of a covered cyber incident can disrupt their incident response, impose unnecessary cost, and inundate CISA with a large amount of data unrelated to an actual incident. Scoping the requirement to confirmed incidents ensures that only substantial cyber incidents are reported, reducing the reporting burden on covered entities and the intake process within CISA.

This also is consistent with CISA's intent of collecting information on actual substantial cyber incidents. Collecting information on actual incidents will help prevent CISA from being overwhelmed with information and will ensure that the information that CISA receives is quality.

4. Submitting Reports

The proposed regulations indicate that submissions will need to be made through a CISA portal. CISA provides examples of other technologies that it has chosen to not implement at present; however, we urge CISA to allow other methods of submission as quickly as possible.

The proposed regulations specifically preclude email submissions. DHS cites the difficulty in its ability to ingest secure email submissions. However, there are ample technologies in the market that enable organizations to accept secure email into ticketing systems. Email submissions provide substantial benefits to covered entities who are submitting incident reports; key among these is that they provide the opportunity for legal review of the submission. Standard incident response procedures include close engagement and coordination with internal legal counsel.

This is especially the case when a company is ensuring compliance with a vast number of regulations and incident reporting mandates across various state, federal, and international governments. Requiring a web-based submission process with unpredictable and unknown questions, as described in the proposed regulations, will prevent adequate legal review of a company's submission. This exposes companies and, potentially the submitter, to greater liability. It is especially important to have this legal review because the submitted information will be shared across the federal enterprise, including with other regulatory agencies. Furthermore, it is a matter of fairness that when an entity is potentially liable for the information being submitted, it should have the opportunity to engage legal counsel prior to making the submission.

We also ask for clarification as to when an incident is "mitigated or resolved." Is an incident fully resolved when actions are taken that protect the covered entity from the incident they are experiencing? Or is the incident "mitigated or resolved" only after all consequences are addressed?

For example, assume a vulnerability was exploited to disrupt business operations and prevent a company from providing goods or services to its customers. Is the incident "mitigated and resolved" once the fix is deployed for that vulnerability and full business operations are restored? Or is the incident "mitigated and resolved" only after any customer impact issues are resolved?

We submit that, for purposes of CIRCIA, the reporting requirements end once the network is protected from the attack. Although other aspects of consequence management might be ongoing (communicating with customers, providing them accommodations for the disruption, etc.), the actual incident is resolved once the network is protected, the adversary no longer has access to the network, and business operations are restored.

5. Third Party Submissions

We appreciate that the regulations enable third parties to submit the required incident reports on behalf of the covered entity. It was referenced specifically that this function could be filled by a sector-specific ISAC.

We ask, however, that the regulations take a more expansive view of this provision and enable a covered entity to conduct joint submissions. One goal of an expanded approach would be to enable a covered entity to submit incident reports to its ISAC and have that information be forwarded to CISA. This way the ISAC and its members will have quick access to information on an incident that occurred within that sector.

For example, if CISA will only enable electronic submissions via a web-based platform (which we caution against for the reasons described above), we propose that the webform provide the submitter with the option for CISA to immediately share the incident report with the sector's Information Sharing and Analysis Center. If the goal of mandatory incident reporting is to provide critical infrastructure owners and operators with actionable threat intelligence, sharing this information directly with industry-specific ISACs so that they can analyze the information and distribute it throughout the sector will facilitate this goal. Of course, this does not prevent CISA from ingesting the report, reviewing it, and producing its own analysis.

This could also work for other submission methods, once DHS enables them. A covered entity could provide an incident report to the ISAC, which can then be forwarded via email to CISA. Another option would be to leverage automated tools for such sharing.

6. Protection and Distribution of Information

While we understand that there will, at times, be a need for CISA to share incident reports with partners in industry and government, we would like to emphasize the vital importance that these reports and the sensitive information they contain are protected to the highest extent possible. This information would be a highly attractive target for a large number of threat actors, and CISA itself has already experienced an incident against one of its more sensitive platforms.

The proposed regulations provide CISA with the ability to share incident reports far and wide. To protect the victim, at minimum, incident reports shared beyond CISA should not identify the covered entity that reported the information. Certain information CISA is required to collect—such as the amount of ransom paid and its currency—does not have security value and should not be included when these reports are shared beyond CISA.

We appreciate that the regulations confirm that these reports are not subject to Federal or State Freedom of Information Act (FOIA) laws. However, we do not see where the proposed regulations identify any additional safeguards for protecting the incident reports and the information in them. For example:

- What authority does CISA have to ensure the reports are securely stored and protected appropriately across the agencies that will receive them?
- Who in the federal enterprise will have access to these incident reports?

- What penalties, if any, will be imposed for unauthorized disclosure of such information?
- What is the process CISA will follow to notify an entity if any of the information it submitted was accessed without authorization?
- What rules will be in place to govern the sharing of information within the government?
- Will the entire incident report be shared throughout the federal enterprise, or will CISA share streamlined reporting/analysis that strips certain information from the reports to protect the victim company?
- How long will the incident reports be held by CISA, and how will they ensure the reports are properly destroyed after that time?

Finally, the proposed regulations state:

> *Information provided to CISA in a CIRCIA Report or in a response to a request for information issued under § 226.14(c) may be disclosed to, retained by, and used by any Federal agency or department, component, officer, employee, or agent of the Federal Government, consistent with otherwise applicable provisions of Federal law, solely for the following purposes:*
>
> *(i) A cybersecurity purpose;*
>
> *(ii) The purpose of identifying a cybersecurity threat, including the source of the cybersecurity threat, or a security vulnerability;*

We have several questions about the "agent of the federal government":

- What is an "agent of the federal government?" We were unable to find a definition for this term.
- What obligations are on "agents of the federal government" to adhere to FOIA and other protections?
- If these agents are private sector contractors, what limits, if any, are on their use of this information?
- Are they able to receive incident reports submitted by a competitor or non-public information that relates to a competitor?
- What recourse do entities whose information is inappropriately shared or used have?

7. Request for Information

The proposed regulations state: *"The Director may issue a request for information to a covered entity if there is reason to believe that the entity experienced a covered cyber incident or made a ransom payment but failed to report the incident or payment in accordance with § 226.3."*

There are several concerns related to this "reason to believe" threshold. First, it is unclear whether the RFI can be submitted only if the CISA Director has "reason to believe" an incident has occurred, or if anyone in CISA has "reason to believe." For example, if a government official inspecting a facility overhears chatter about a "cyber incident" or a "network being down" and then reports that to a regional CISA cybersecurity advisor, is that sufficient "reason to believe?"

We submit it is not. Rumor and innuendo might be believable, but that should not meet the "reason to believe" threshold. CISA itself has long warned of mis- and disinformation campaigns, and it is not hard to envision scenarios in which false information is spread about a company. To avoid abuse, CISA should impose guardrails, to include banning third party reports from anonymous, unverified sources and setting transparent thresholds as to what constitutes a "reason to believe."

Defining what triggers a “reason to believe” is vitally important as CISA seeks to balance its role as a partner and regulator. Discussions about threats, threat actors, and routine voluntary sharing and collaboration among CISA and industry analysts could be chilled if CISA uses these forums as a means to glean whether a covered entity has experienced an attack. If CISA determines it has a “reason to believe” a reportable incident has occurred based on these routine, collaborative discussions, then this likely will reduce the voluntary collaboration between industry and government.

Relatedly, CISA should further clarify what constitutes an “inadequate” response within 72 hours of an organization receiving a RFI that would permit the director to issue a subpoena. Good faith cooperation should not qualify as “inadequate,” and should also be a factor in determining whether a subpoena is necessary. Additionally, the scope of information that CISA could attempt to compel through subpoena should be clearly defined within the Proposed Rule.

8. Preservation of Evidence

Asking companies to preserve information for two years after the incident is resolved is a costly mandate with no apparent value to industry. If law enforcement or government wants to preserve the information, it should assume the cost and responsibility of preserving the information, not the victim enterprise. At a minimum, CISA should reduce the data preservation requirement to 1-year, which we believe is a sufficient timeframe that will allow a covered entity to conduct analysis of the incident and for CISA to determine if the incident is related to other incidents or of sufficient value to the U.S. Government to conduct follow up inquiries.

Conclusion

Finally, we would like to take this opportunity to again note the importance of harmonizing the multitude of cybersecurity regulations and reporting requirements. Bringing consistency to these reporting requirements will drive down compliance costs and allow organizations to dedicate more of their limited resources to security.

The IT-ISAC and the IT-SCC appreciate the opportunity to present our comments. We believe that with these recommendations and clarifications, these regulations will be more manageable and helpful to both CISA and the organizations it seeks to protect. We thank you for your consideration.