Comments by the Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG) on the DHS "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements"

Docket No. CISA-2022-0010, RIN 1670-AA04, https://federalregister.gov/d/2024-06526

Comments due July 3rd, 2024

I. Introduction

The Messaging, Malware, and Mobile Anti-Abuse Working Group (M[3]AAWG, https://www.m3aawg.org/) appreciates the opportunity to submit these comments on the above-referenced draft rulemaking proceeding ("NPRM"). M[3]AAWG is a technology-neutral global industry association. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. With more than 200 institutional members worldwide, we bring together stakeholders in the online community, developing best practices and cooperative approaches for fighting online abuse.

M[3]AAWG recognizes the key role effective cyber incident reporting can have in addressing the impacts of cybersecurity incidents and combating online abuse. Cyber incident reporting can minimize consequences to victims, capture lessons learned, and improve cybersecurity nationwide, thereby increasing the likelihood that perpetrators will be held accountable. However, overly broad cyber incident reporting rules often do not, on balance, yield benefits commensurate with the significant costs those rules impose on both reporting entities and the government.

We generally support CISA's efforts to craft a proposed rule that seeks to achieve the intended goals of the CIRCIA mandates. However, M[3]AAWG urges CISA to consider the following suggestions to clarify or modify its proposed rule, as detailed below. We note that our comments today are focused on certain critical areas of concern to our members and do not represent a comprehensive discussion of all issues covered in the expansive CIRCIA NPRM.

II. Discussion

A. CISA should reconsider *which organizations* are required to report.

CISA's definition of "Covered Entity" is excessively broad.

> *"The overwhelming majority of entities, though not all, are considered part of one or more critical infrastructure sectors. Illustrative examples of entities that generally are not considered part of one or more critical infrastructure sector include advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups."*
> -- 89 FR 23678

This definition appears to expand the scope of covered entities beyond the typical organizations that are considered part of CISA's 16 critical infrastructure sectors. It includes entities that may be adjacent or tangential to – but not integral to – critical infrastructure. Capturing the majority of entities in a definition of critical infrastructure for purposes of cyber incident reporting:

- requires these organizations to implement and establish costly reporting capabilities;
- exposes these organizations to potentially significant regulatory liability;
- stretches scarce resources that are focused on managing the attack and identifying and mitigating threats, and;
- substantially increases the volume of reports submitted in cases where there are limited connections to critical infrastructure cybersecurity.

M[3]AAWG recommends that CISA significantly refine the entities subject to the rule, and then potentially extend the definition as appropriate after an initial roll-out period is completed.

B. CISA should reconsider and clarify *what sorts* of cyber incidents must be reported.

As with the definition of "Covered Entity," CISA's proposed scope of a reportable "Covered Cyber Incident" is excessively broad. A "covered cyber incident" is defined "to mean a substantial cyber incident experienced by a covered entity." See 89 FR 23660. A substantial cyber incident is:

> *"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." --89 FR 23661*

In addition, the proposed rule uses terms that are vague, subjective, and lack clarity. Examples that are meant to be illustrative of what is or is not a substantial or minor cyber incident contain language that is unclear, which leads to varied interpretations and judgment calls by reporting entities. Terms such as "an extended period of time," "brief period of unavailability," "short-term unavailability," "temporary need," "quickly detected," and "significant additional activity" (see 89 FR 23668) are subjective. When considering duration, does it also matter when the incident occurs? Some incidents may have more impact if they occur during major events, even if they are brief in duration. Similar questions could apply to other terms. We recognize, as CISA notes, that there may be instances where case-by-case analysis is required. However, if CISA's intent is to be overly inclusive with respect to reportable cyber incidents at the outset (which we do not recommend), case-by-case instances should be few and far between. Therefore, M[3]AAWG recommends that CISA:

- clarify and define key terms;
- work towards adoption of "bright line" objective criteria on what is and what is not subject to mandatory reporting;
- specify exact date ranges, and;
- be clear on expectations for incident impact timeframes.

Finally, in the NPRM, CISA claims its intent to collect such information is to:

> *"provide the Federal government with enhanced cross-sector visibility into the cyber threat landscape and support the aggregation, analysis, and sharing of incident data in a way that heretofore has been unavailable to the cybersecurity community. This, in turn, would facilitate a better understanding by both Federal and non-Federal entities of who is causing cyber incidents; what types of entities malicious cyber actors are targeting; what tactics, techniques, and procedures malicious cyber actors are using to compromise entities in critical infrastructure sectors; what vulnerabilities are being exploited; what security defenses are effective at stopping the incidents; and what mitigation measures are successful in reducing the consequences of an incident."*
> *--89 FR 23750*

We caution that such an extensive data collection is likely to have the opposite effect and will likely decrease the signal-to-noise ratio so critical to pattern identification and threat awareness.

C. CISA should clarify report timeline expectations.

In the NPRM, CISA notes:

> *"CIRCIA requires covered entities to report to CISA covered cyber incidents within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred and ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made."*
> *--89 FR 23648*

CISA also notes that it

> *"…recognizes that potential drawbacks to over prioritizing timely reporting exist, such as potentially impacting a covered entity's ability to conduct preliminary incident response and mitigation. CISA also recognizes that a covered entity may not have all the information in the early aftermath of incident discovery, and that some preliminary determinations made at the outset of an incident response process may later be determined to be inaccurate when the entity is afforded time to conduct further investigation and analysis. Accordingly, CISA has sought to balance the critical need for timely reporting with the potential challenges associated with rapid reporting in the aftermath of a covered cyber incident."*
> *--89 FR 23653*

M^{3}AAWG concurs with this assessment. Given the complexity of cyber incidents, the entity being subjected to the attack may not even know they have been compromised until well into the actual attack. Even if there were some indicators that triggered an investigation, the verification can take days or weeks in some cases, and sometimes longer to determine the full scope of the impacted systems.

While CISA declines to define "reasonable belief" in a rule, it proposes to include guidance in the text of its final order. Such guidance acknowledges that "an entity may need to perform some preliminary analysis before coming to a 'reasonable belief' that a covered cyber incident has occurred"; "this preliminary analysis should be relatively short in duration (i.e., hours, not days)...and generally would occur at the subject matter expert level and not the executive officer level"; and that "confirmation" is not required before the 72-hour reporting timeframe is triggered. See 89 FR 23725. CISA also allows covered entities to submit new or updated information in a supplemental report.

M^{3}AAWG urges CISA to allow regulatory flexibility regarding timeline expectations, within the constraints of statutorily mandated timeframes for required filers, by, for example, phased reporting for critical incidents, and allowing at least ten business days for investigation and filing of reports.

D. CISA should harmonize cyber incident reporting requirements.

Covered entities should also not be required to engage in redundant or duplicative cyber incident reporting. As CISA itself acknowledges:

> *"Given the number of existing cyber incident reporting requirements at the Federal and SLTT levels, CISA recognizes that covered entities may be subject to multiple, potentially duplicative requirements to report cyber incidents. In an attempt to minimize the burden on covered entities potentially subject to both CIRCIA and other Federal cyber incident reporting requirements,* ***CISA is committed to exploring ways to harmonize this regulation with other existing Federal reporting regimes,*** *where practicable and seeks comment from the public on how it can further achieve this goal."* [emphasis added]
>
> --89 FR 23653

We concur with this sentiment and recommend that harmonization efforts consider coordinated information sharing among relevant agencies and access opportunities as appropriate.

E. CISA should reduce the required retention period.

M[3]AAWG also urges CISA to reduce the required information retention periods. Currently CISA proposes a two-year retention period for records relating to a covered incident. We believe that timeframe is excessive, and will likely substantially burden and add extensive costs to covered entities. The initial retention period should only be as long as necessary to allow an interested agency to issue a specific record retention demand, should that information be needed. We propose that CISA consider adoption of a six-month period. If an agency does not lodge a specific retention demand during that six-month period, *and* the impacted entity does not require retention for other purposes (such as, but not limited to, potential civil litigation or insurance-related purposes), record retention should be at the covered entity's discretion after the six-month window has passed.

F. CISA should reconsider sole use of a web-based form for report submissions.

CISA proposes that covered entities must *"*[...] submit CIRCIA Reports through the web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner approved by the Director." CISA further states that "[o]n balance, CISA believes that the web-based form is the most useful and cost-effective manner for the submission and receipt of CIRCIA Reports and is proposing that as the sole explicitly identified option for submission of CIRCIA Reports." See 89 FR 23714.

We have concerns about the use of a web-based form as the sole and primary option for report submission. These include, but are not limited to, the concerns discussed below.

- Web-based form solutions are attractive and familiar targets, vulnerable to attacks on the underlying protocols and potentially prone to DDoS attacks, SQL injection attacks, and service/software compromise, among others.
- Manually populating reporting web forms will be very slow. CISA states at 89 FR 23745 that:

  > *CISA estimates that both Covered Cyber Incident and Ransom Payment Reports would take three hours to complete, a Joint Covered Cyber Incident and Ransom Payment Report would take 4.25 hours to complete, and a Supplemental Report would take 7.5 hours to complete.*

  Assuming these estimates are accurate and not underestimated, submissions that take that long to complete simply do not scale. These time frames could be significantly longer if covered entities are forced to

complete the report using a web browser on a smart phone in the event the cyber incident prevents access to the operational systems that would have otherwise enabled the required reporting.

- CISA also "intends to maintain a capability to support reporting via telephone as a back-up option" during temporary unavailability of the web-based form portal. See 89 FR 23714. Such a telephonic backup as proposed by CISA is also unrealistic and unscalable.

- CISA envisions "submission of digital artifacts" such as "malware samples." We urge CISA to take appropriate care when intentionally collecting malware samples (and malicious URLs) to avoid inadvertent infection of the collection portal and to segregate malware (and malicious URLs) from other content to the maximum extent possible.
- CISA states at 89 FR 23714 that "[...] a cyber incident at a covered entity could make it impossible or insecure for a covered entity to use its own information system(s) to report via a web-based form. CISA believes that this is a relatively minor concern, however, as organizations and individuals today typically have a variety of ways to access the internet." We disagree. Some entities may not have as many internet access options available to them or be able to manage potentially costly third-party submissions. Because incidents may involve Federally-classified information, a classified web portal will be needed in order to be able to accept reports involving classified content. Those classified servers will not normally be accessible from the public internet. If access to those servers is limited to just classified agency networks (such as SIPRNet or JWICS), incidents *involving* those networks may cause a circular dependency: the network is compromised (and must be reported to the classified CIRCIA portal), but the only connection to the classified CIRCIA portal would be over the potentially-insecure classified network connection.

M^{3}AAWG urges CISA to reconsider its decision to postpone automated (i.e., machine-to-machine) reporting until the future (see 89 FR 23714). M^{3}AAWG does recommend that CISA consider a RESTful API interface that allows for a new cyber incident report, or for appending information to an already existing report.

With respect to the content of a cyber incident report, we recommend that the exact fields required should be clearly identified and versioned (so that updates and changes can be tracked and submissions can show that they satisfied all requirements that were necessary at the time of submission, even if those requirements may have changed since that point).

G. CISA should ensure adequate mechanisms to protect compelled defensive data from disclosure.

Cybersecurity relies upon informational asymmetries as one of the only advantages to the defender in a hostile operating environment. We recognize that the interests of the U.S. government may be served in the short-term through compelling disclosure of cyber-attack details, defender posture, countermeasures in place, exact versions of software deployed, practices used to limit scope of an attack, and mechanisms or technologies helpful in identification and isolation of those attacks. That said, we strongly urge CISA to ensure that such sensitive, potentially confidential information be adequately protected from disclosure through data breaches or other encroachment by adversarial entities. This is because these reports, coupled with other available information (e.g., software bill of materials [SBOM) and common vulnerability and exposure [CVE) databases) and tools such as Metasploit, nmap, and open-sourced attack frameworks have automated the attack infrastructure such that merely knowing the software and version can yield an effective attack framework, can provide a roadmap of what to attack, how to attack it, and a toolkit enabling automation of those attacks. The advent of some newer generative AI tools have further advantaged the attackers and made these threats increasingly economically viable.

III. Conclusion

As noted above, we generally support CISA's efforts to craft cybersecurity incident reporting rules to the extent that these rules are sufficiently clear, balanced, effective, and narrowly tailored to achieve the desired objective.

We appreciate the opportunity to submit these comments, and we welcome further opportunities to engage as needed to answer any questions during this process. Please address any inquiries to M^{3}AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,

Amy Cadagin
Executive Director
Messaging Malware Mobile Anti-Abuse Working Group
comments@m3aawg.org
P.O. Box 9125, Brea, CA 92822