NOTICE OF PROPOSED RULEMAKING

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

Docket #: CISA-2022-0010

July 3, 2024

I. INTRODUCTION

In response to the Cybersecurity and Infrastructure Security Agency's ("CISA") proposed rulemaking required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("proposed rule") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike strongly supports the proposed rule's goal of better protecting U.S. critical infrastructure, and citizens, from cybersecurity threats. These threats continue to evolve and grow more severe. In a recent report, for example, we found that government agencies and related entities remained top targets for cyber attacks in the past year.[1] Furthermore, the report found that nation-state adversaries were active throughout 2023, and continued to operate at an unmatched pace, leveraging stealth and scalable techniques to collect targeted group surveillance data, strategic intelligence, and intellectual property.[2] Some of these groups have demonstrated the capability of leveraging disruptive or destructive cyber attacks to effectuate political or

[1] *2024 Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/
[2] Ibid.

policy aims. This makes steps to enhance cybersecurity across critical infrastructure sectors timely and appropriate.

It is clear that CISA drafted the proposed rule taking into consideration previous stakeholder feedback, which we appreciate. While we do not have feedback on every aspect of this proposed rule, we do want to offer several points that may be of value to CISA's final rulemaking.

A. Definitions

Fundamentally, incident reporting obligations are often resource intensive, especially for small entities, and can result in tradeoffs. Accordingly, CISA should endeavor to achieve balance in scoping covered entities and incidents. The volume of resulting reports should be sufficient to discover and alert entities about systemic and/or widespread threats; but not be so great as to create "noise" for analysts and extra work for those affected by low-impact commodity threat activity. As currently drafted, the scope of both covered entities and covered incidents are potentially too broad to achieve this aim.

Definition of covered entity. It is important to ensure that organizations whose disruption could have national-level or sector-wide implications are in scope. However, it's worth considering whether additional consideration might be extended to small enterprises in particular. Based on our experience performing incident response services for a variety of cyberattack victims, small entities confront significant constraints during remediations. In some cases, satisfying reporting obligations may divert resources and attention from the incident remediation process itself. This, in turn, could amplify the impact of the incident. Rather than relaxing the 72 hour reporting window, which is rapidly emerging as a common timeframe, it may be worth revisiting whether entities below a certain size threshold (which may thus be disproportionately impacted by regulatory obligations) might be excepted from the "covered entity" criteria.[3]

Definition of covered incident. In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and regulations. In most cases, organizations using contemporary cybersecurity solutions are alerted to malicious activity occurring in their environment. The nature of these alerts may vary, and could cover something like the installation of malicious software on one system, or

[3] Please see section "C," *Impact on Small Entities* below.

the compromise of a single account. In scenarios where defenders see these alerts and address them quickly, the alert may not rise to the threshold of a cybersecurity "incident," where the threat actor has not meaningfully achieved their objective, accessed sensitive information, and the like.

As such, CrowdStrike agrees with CISA's decision to have a covered incident only be a "substantial cyber incident." However, CISA should consider further amending the covered incident definition (§ 226.1) to focus on outcomes. As written, Sections (1), (2), and (3) attempt to use this approach. However, Section (4) focuses on specific attack vectors that shift meaningfully over time, leading to a nebulous definition. To the extent that a threat actor uses those means–or other standard or emerging means–to achieve any of the conditions outlined in the previous sections, that should trigger a reporting obligation.

Definition of supply chain compromise. Currently, the definition of supply chain compromise includes potential incidents. There are significant distinctions between cybersecurity alerts and incidents[4], and reporting of issues mitigated or resolved at the alert-level is unlikely to provide additional value. As noted above, the attack vector should not be a predicate for a covered incident; the outcome of the attack should determine reportability regardless of the means.[5]

B. CIRCIA Agreements

The proposed rule introduces the concept of a "CIRCIA Agreement" or a relationship between CISA and another Federal agency where reporting to CISA satisfies both agency's reporting requirements. CrowdStrike applauds this initiative. Streamlining reporting, where possible, can make reporting an incident easier for a victim while they are trying to respond to an attack.

To the extent practical, CISA should negotiate CIRCIA Agreements concurrently with the final rule's development. This would ensure that agreements are in place when requirements go into effect for covered entities. CISA should negotiate as many CIRCIA Agreements as possible, including with independent agencies.

---

[4] Described in "*Definition of covered incident.*"

[5] If CISA retains obligations to report supply chain compromises, a more appropriation definition might be: "*Supply chain compromise means a cyber incident within the supply chain of an information system that an adversary* ***leverages*** *to* ***substantially*** *jeopardize and* ***seriously impact*** *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.*"

C. Impact on Small Entities

Of the 316,244 covered entities, CISA estimates that 310,855 would be considered small entities. As noted above, based on our experience working with impacted entities, it may be reasonable to make an exception for entities below a certain threshold, so they may focus on remediation when dealing with an incident.

Additionally, the proposed rule has a section titled "Assistance for Small Entities." In that section, there are no meaningful opportunities for small entities to obtain assistance from CISA. In other words, there is a new compliance regime applicable to small entities without a clear means for them to meet such requirements. If CISA proceeds with the final rule without a carveout for small entities, CrowdStrike recommends that CISA prepare tailored outreach, and design trainings to educate and assist small entities with compliance to CIRCIA.

III. CONCLUSION

CISA's proposed rule on CIRCIA represents an important step forward for critical infrastructure security. We hope that industry stakeholders, including potential covered entities, have continued opportunities to voice comments as the implementation process continues. Finally, because cybersecurity capabilities – both of the defenders and adversaries – evolve faster than law and policy, we recommend that any legislative updates and proposed rulemaking focus on principles, where appropriate, rather than prescriptive requirements and include mechanisms for periodic review, updates, and revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***