CROWDSTRIKE

REQUEST FOR INFORMATION RESPONSE

Cyber Incident Reporting for Critical Infrastructure Act of 2022

November 14, 2022

I. INTRODUCTION

In response to the Cybersecurity and Infrastructure Security Agency's (CISA) request for feedback on proposed regulations required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), 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

We appreciate CISA's engagement efforts - including this Request for Information (RFI) and the listening sessions - to reach a variety of stakeholders throughout this process. We have included responses to specific RFI questions, along with general observations and comments that may be useful in the implementation of CIRCIA.

A. Definitions, Criteria, and Scope of Regulatory Coverage.

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 incidents; but the volume should not be so great as to create "noise" for analysts and extra work those impacted by low-impact commodity threat activity.

Definition of covered entity. The underlying statute clarifies that the definition of covered entity means "an entity in a critical infrastructure sector, as defined in Presidential Policy

Directive 21."[1] While this is an important clarification, the definition of critical infrastructure is still broad. We recommend that CISA further clarify the definition of covered entity to focus on entities whose disruption would potentially cause catastrophic or systemic impacts.

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 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 recommends that a covered incident only be defined as a substantial cyber incident and CISA not create a distinction between the two.

CrowdStrike recommends that a covered cyber incident be defined as an substantial cyber incident that meets the following criteria:

- An undesired effect on an IT, OT, or other digital system within a covered entity that adversely and materially impacts the operations or provision of critical services, or
- The material loss of, compromise in, or sustained denial of access to non-public data, intellectual property, or trade secrets within a covered entity that adversely impacts the provision of critical services, homeland security, or national security, or
- Systemic impacts to critical infrastructures/services relied upon by the covered entity to provide core critical infrastructure functions.

B. Report Contents and Submission Procedures

Report contents. From the responses to the RFI, and other stakeholder engagements from entities that likely will be covered by implementing regulation, CISA should develop a draft of the data fields asked in the reporting mechanism and a workflow of the submission procedures. We recommend that CISA release a draft version of the data fields and forms to industry for another round of stakeholder engagement – whether that be through a

[1] Presidential Policy Directive 21 defines "critical infrastructure" as section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)): "namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Request for Comment period or workshops. Without proposed data fields or a draft template to respond to, it is difficult for organizations to envision the types of information that is most useful to CISA. Furthermore, it is important to consider forthcoming harmonization recommendations resulting from the ongoing work of the Cyber Incident Reporting Council, which was created by CIRCIA to harmonize the many existing federal cyber incident structures and requirements.

Submitting reports. Once the report contents are resolved, to the extent possible, CISA should make available a variety of reporting formats to fit the needs of different covered entities. While certain information should be mandatory to report, as determined through the stakeholder engagement efforts, digital report formats can allow CISA to gather additional fields of information. CISA should explore creating workflows that would allow victim organizations to explicitly permit CISA to refer reports to other regulators to streamline other reporting requirements or obligations.

Reasonable belief. Not all cyber incidents have the same level of severity and rise to the level of "substantial" to be reported. For example, an incident where a threat actor gains access but is not able to move laterally due to strong security practices likely would have a minor impact on the covered entity. Whereas, another incident in which a threat actor infiltrates, moves laterally, and is able to control OT systems may have a severe impact. While these are important distinctions, the two incidents could look similar in the early investigation stage. Consideration of the impact and severity of an incident is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures. Consequently, it is extremely difficult, if not impossible, to create a threshold of when reasonable belief of a cyber incident is reached that could be applied across various types of incidents. As a part of the rule making progress, CISA should develop guidance, such as case studies, for covered entities as to what it believes is "reasonable" in varying circumstances to ensure entities are in a position to best comply with the requirements of the act.

Third party reporting. First, we recommend that CISA confirm that there is no affirmative third party reporting requirement and that third party reporting occurs *only if* a covered entity enters into a contract with a third party to report *on the covered entity's behalf*. Today, many entities rely upon third parties such as cybersecurity companies, incident response providers, law firms, insurance providers or information sharing and analysis organizations to comply with notification obligations. Further guidance should reiterate, as the statute lays out, that the "duty to report" is the responsibility of the impacted covered entity.

Second, we recommend that CISA clarifies that the intent of the statute is to allow third party cybersecurity companies, incident response providers, law firms, insurance providers or information sharing and analysis organizations to submit a covered cyber incident report on behalf of a covered entity that has been impacted by a cyber incident and is subject to the requirements under § 2242 – at the covered entities request. Small- and medium-sized businesses, as well as other entities that ultimately end up being considered "covered entities," might not have the resources or capabilities to comply with the requirements in a timely manner. Allowing third parties to report on their behalf will give these entities the opportunity to leverage the expertise of incident response providers, law firms, insurance providers, and others.

In terms of guidelines and reporting, we recommend that the guidelines and procedures for third party submissions be consistent with the reporting mechanisms, guidelines, and procedures as those established for covered entities reporting cover cyber incidents, as determined by the rulemaking process.

As described in the RFI, an "incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm" constitutes the bulk of the third party entities. However, this should not be an exclusive list. Other types of organizations such as non-profits or Information Sharing and Analysis Centers (ISAC's) could be asked to report an incident on behalf of a covered entity.

We understand that third party advisors are required to advise covered entities on their ransom payment reporting responsibilities. Given significant variation in contracting arrangements, specific terms should be outlined between a third party and the covered entity during their contractual negotiations rather than in regulations.

C. Other Incident Reporting Requirements and Security Vulnerability Information Sharing

Vulnerabilities. Within the private sector, longer-term vulnerability disclosure norms have emerged. For example, in general, security researchers make a 90 day allowance following the discovery and reporting of a vulnerability in another vendor's software.[2] Even when vulnerabilities are being actively exploited, organizations typically have seven or more days before the researcher makes a disclosure. Exacerbating factors where public notice could be detrimental to an ongoing incident response investigation include, for example, when data extortion is at play, a law enforcement investigation mandating confidentiality, or where it may take additional time to incorporate the preventative measures necessary to

[2] *See generally*, Tim Willis, *Project Zero* (Apr. 12, 2021), https://googleprojectzero.blogspot.com/2021/04/policy-and-disclosure-2021-edition.html.

prevent an even more significant impact (such as in vulnerability disclosure). We recommend CISA align any vulnerability regulations with these best practices.

Attorney-Client Privilege. An additional point that CISA should consider is attorney-client privilege between covered entities and any legal teams they may employ for incident response. As noted in § 2245(b) of CIRCIA, reports describing covered cyber incidents or ransom payments shall be considered commercial, financial, and proprietary information of the covered entity and not be considered a waiver of any applicable privilege. As CISA has noted, when organizations respond to an incident, they often work with attorneys and incident response teams under attorney-client privilege and it is key to maintain a level of trust and confidentiality in order navigate regulatory requirements, complete a thorough investigation, and ultimately foster meaningful reporting.

III. CONCLUSION

CISA's RFI on CIRCIA represents an important step forward as incident reporting for Critical Infrastructure is implemented. We hope that industry stakeholders, including potential covered entities, have continued opportunities to voice comments as the implementation process continues. Finally, because the underlying technologies and adversary TTPs evolve faster than law and policy, we recommend and emphasize 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® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about 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

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***