hackerone

June 28, 2024

VIA ELECTRONIC SUBMISSION

Re: HackerOne Response to Request for Comment on the Cyber Incident Reporting for Critical Infrastructure (CIRCIA)

Dear Sir or Madam:

HackerOne Inc. (HackerOne) submits the following comments in response to the Cybersecurity and Infrastructure Security Agency's (CISA) proposed regulation implementing the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) reporting requirements.[1] We appreciate the opportunity to provide input, and we commend CISA for aiming to promote stronger cybersecurity standards across critical infrastructure entities.

By way of background, HackerOne is the global leader in human-powered security. We leverage human ingenuity to pinpoint the most critical security flaws across your attack surface to outmatch cybercriminals. The HackerOne Platform combines the most creative human intelligence with the latest artificial intelligence to reduce threat exposure at all stages of the software development life cycle. From meeting compliance requirements with pentesting to finding novel and elusive vulnerabilities through bug bounty, HackerOne's elite community of ethical hackers helps organizations transform their businesses with confidence. HackerOne has helped find and fix more vulnerabilities than any other vendor, for brands including Coinbase, General Motors, GitHub, Goldman Sachs, Hyatt, PayPal, and the U.S Department of Defense.

We believe that effective incident reporting is crucial for understanding and mitigating cyber threats, and we support CISA's efforts to create a robust framework for timely and efficient reporting. We also recommend, however, that the regulations be designed in a way that minimizes the compliance burden on organizations, allowing them to focus on swift recovery and resilience building post-incident.

Below HackerOne provides feedback and suggestions on how to improve the proposed CIRCIA rule:

[1] Proposed Rule Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements, Cybersecurity and Infrastructure Security Agency, 89 Fed. Reg. 23644, Apr. 4, 2024, https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

I. Revise the Definition of Covered Cyber Incidents.

The proposed rule defines "covered cyber incident" to include "all substantial cyber incidents experienced by a covered entity."[2] While CIRCIA does not define "substantial cyber incident", it provides minimum requirements for the types of substantial cyber incidents that qualify as covered cyber incidents. Instead of this approach, we suggest CISA leverage CISA's National Cyber Incident Scoring System and the National Critical Functions, and define "covered cyber incident" to include substantial cyber incidents that results in impact on public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.[3]

By revising the definition of covered cyber incident, CISA can ensure that resources are focused on incidents with significant implications. Taking a risk management approach will help focus the limited resources of CISA, avoid overwhelming incident responders and reduce the volume of less actionable reports.

II. Clarify the Exclusion for Good Faith Security Research

CISA proposes that a covered cyber incident excludes "any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system… such as in accordance with a vulnerability disclosure policy or bug bounty programs."[4]

We support and appreciate CISA's effort to carve out authorized good faith security research from the scope of covered cyber incidents. However, we encourage CISA to clarify that this independent good faith security research as a whole does not trigger a CIRCIA Report requirement. We are concerned that good faith security research that falls outside the scope of express authorization for vulnerability disclosure program (VDP) or bug bounty program (BBP) may not be excluded by this language, as such activity may not be considered to be in response to a "specific request" by the covered entity.

Independent good faith security research often involves proactive efforts by researchers to identify vulnerabilities and enhance cybersecurity without prior solicitation by companies. It is crucial to also explicitly recognize and exclude good faith security research that may occur independently, without a prior request, but aims to identify and remediate vulnerabilities for the benefit of the information system owner or operator. This broader exclusion would support the valuable work of independent security researchers who often perform unsolicited work to enhance the safety and security of digital infrastructure.

---

[2] 89 Fed. Reg. 23644, 23661.
[3] CISA National Cyber Incident Scoring System, Sep. 30, 2020, https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss.
[4] *Id.*

III. Ensure Harmonization and Reciprocity in Incident Reporting

Harmonization and reciprocity of cyber incident reporting requirements are critical for reducing the compliance burden on organizations and enhancing the overall effectiveness of cybersecurity efforts. While we recognize the benefits of incident reporting, redundant and overlapping reporting requirements risk overwhelming response teams and diluting the focus on critical threats.

As a result, we strongly encourage CISA to work with its federal and non-federal partners to mitigate the challenges posed by the varying cyber incident reporting requirements across different jurisdictions. Congress recognized the importance of doing so and directed the Department of Homeland Security (DHS) to establish a Cyber Incident Reporting Council (CIRC), a committee of federal agencies to coordinate, deconflict and harmonize existing and future federal cyber incident reporting requirements. The CIRC's report, "Harmonization of Cyber Incident Reporting to the Federal Government," highlights that there are 52 cyber incident reporting requirements in effect or proposed at the federal level alone, not including state, local, tribal, or territorial (SLTT) jurisdictions.[5]

Under CIRCIA, CISA has the authority to reduce duplicative reporting requirements through the "substantially similar" exception.[6] However, the proposed rule is not clear regarding the criteria CISA will use to determine what qualifies under this threshold and whether less detailed requirements would be permissible.[7] We urge CISA to embrace reciprocity by accepting all federally mandated cyber incident reports as compliant with CIRCIA, and by proactively requesting supplementary information when necessary to ensure comprehensive reporting and effective cybersecurity response.

Finally, we support the proposed requirement for a unified, web-based interface for all CIRCIA reports.[8] This initiative will significantly streamline the reporting process by providing a centralized platform for entities to submit incident reports efficiently. By standardizing the reporting format and enhancing accessibility, this interface will alleviate administrative burdens on organizations and facilitate the timely delivery of critical information to relevant agencies. We encourage CISA to ensure that the proposed system is adequately secured.

* * *

[5] Department of Homeland Security, Harmonization of Cyber Incident Reporting to the Federal Government, Sep. 19, 2023, pg. 9, Appendix B, https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.
[6] 89 Fed. Reg. 23644, 23671.
[7] *Id.*
[8] 89 Fed. Reg. 23718.

HackerOne appreciates the opportunity to provide feedback on the proposed CIRCIA regulation. We believe that by refining definitions, clarifying the exclusions related to independent good faith security research, and prioritizing harmonization and reciprocity, CISA can create a more effective framework for incident reporting. HackerOne remains committed to collaborating with CISA and other stakeholders to strengthen cybersecurity practices and protect digital infrastructure nationwide. Should you have any questions, please contact us at policy-team@hackerone.com.

Respectfully submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne