hackerone

June 24, 2026

VIA EMAIL: CIRCIA@cisa.dhs.gov

CIRCIA Team
Cybersecurity and Infrastructure Security Agency (CISA)

Re: HackerOne Written Materials Submitted in Connection with the CIRCIA Town Hall Meetings (CISA-2022-0010-0469)

Dear Sir or Madam,

HackerOne Inc. (HackerOne) submits the following written materials in connection with CISA's town hall meetings on the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rulemaking, as announced in the Federal Register on February 13, 2026 (91 FR 6794) and rescheduled on May 26, 2026 (CISA-2022-0010-0469).[1] We appreciate the opportunity to provide additional input and commend CISA for continuing to engage stakeholders as it works toward a final rule.

By way of background, HackerOne is a global leader in Continuous Threat Exposure Management (CTEM). The HackerOne Platform unites agentic AI solutions with the ingenuity of the world's largest community of security researchers to continuously discover, validate, prioritize, and remediate exposures across code, cloud, and AI systems. Through solutions including bug bounty, vulnerability disclosure, agentic pentesting, AI red teaming, and code security, HackerOne delivers measurable, continuous reduction of cyber risk for enterprises. Industry leaders including Anthropic, General Motors, Goldman Sachs, Uber, the UK Ministry of Defence, and the U.S. Department of Defense trust HackerOne to safeguard their digital ecosystems.

We believe that effective incident reporting is crucial for understanding and mitigating cyber threats, and we support CISA's efforts to create a robust and efficient reporting framework. These materials build on our June 28, 2024, comments submitted in response to the NPRM and our town hall statement and are offered in the spirit of CISA's stated goal to refine the scope and burden of the proposed rule while preserving the government's visibility into cyber threats affecting critical infrastructure.[2]

1. Revise the Definition of "Substantial Cyber Incident" to Reflect Actual Impact on Critical Infrastructure

The proposed rule defines "covered cyber incident" as "a substantial cyber incident experienced by a covered entity," and proposes a four-part test for what constitutes a "substantial" cyber

[1] *Town Hall Meetings To Provide Input on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Rulemaking*, 91 FR 6794 (Feb. 13, 2026); revised schedule published May 26, 2026, https://www.federalregister.gov/d/2026-10417.
[2] *HackerOne Comments on the CIRCIA NPRM* (June 28, 2024), https://www.hackerone.com/sites/default/files/2025-02/HackerOne-CIRCIA-Comments-.pdf.

incident.[3] The first prong of that test—any "substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network"—is overbroad. As written, it could capture a very wide range of routine or low-severity incidents that pose no meaningful risk to critical infrastructure operations or national security. This risks generating a high volume of reports of limited actionability, overwhelming CISA analysts and diverting resources away from truly significant incidents.

In our June 2024 comments, we recommended that CISA adopt a risk-management approach by leveraging CISA's own National Cyber Incident Scoring System (NCISS) and the National Critical Functions framework to define "covered cyber incident" to include only those substantial cyber incidents that result in material impact on public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.[4] We reiterate that recommendation here.

This approach directly responds to CISA's stated interest in receiving input on "the proposed examples of incidents that likely would or would not qualify as a substantial cyber incident."[5] A definition anchored to actual impact on national critical functions would concentrate both CISA's limited analytical resources and covered entities' compliance efforts on the incidents that matter most, while reducing the volume of low-actionability reports that would otherwise dilute CISA's threat picture.

2. Clarify the Exclusion for Independent Good-Faith Security Research

The proposed rule excludes from the definition of "covered cyber incident" any event "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 program."[6] We supported this exclusion in our June 2024 comments and continue to do so.

However, we remain concerned that the current language does not clearly protect independent, unsolicited good-faith security research (i.e., proactive efforts by security researchers to identify and disclose vulnerabilities without a prior specific request from the system owner). Such research is common, valuable, and consistent with widely recognized responsible disclosure norms. If unsolicited good-faith research can trigger a CIRCIA reporting obligation for the researched organization, the practical effect will be to chill both independent researchers and organizations willing to engage constructively with them. This outcome would be directly contrary to CIRCIA's security objectives.

We urge CISA to explicitly extend the good-faith research exclusion to cover all independent security research conducted in good faith that aims to identify and remediate vulnerabilities for the benefit of the information system owner or operator, regardless of whether that research was

[3] Proposed Rule, Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements, 89 Fed. Reg. 23644, 23661 (Apr. 4, 2024), https://www.federalregister.gov/d/2024-06526.
[4] CISA National Cyber Incident Scoring System, Sep. 30, 2020, https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss.
[5] 91 FR 6794, 6795.
[6] 89 Fed. Reg. 23644, 23661.

initiated pursuant to a specific request. This targeted clarification would support the security research community without in any way undermining CIRCIA's core reporting requirements.

3. Prioritize Harmonization and Adopt a Reciprocity Approach

The February 2026 town hall notice specifically identified "potential approaches to harmonizing CIRCIA's regulatory reporting requirements with other existing federal or state, local, tribal, or territorial (SLTT) laws" and "how to reduce actual, likely, or potential duplication or conflict" as topics of particular interest to CISA.[7] HackerOne has consistently viewed harmonization as one of the most consequential issues in this rulemaking, and we appreciate CISA's continued focus on it.

The DHS Cyber Incident Reporting Council (CIRC) identified 52 cyber incident reporting requirements in effect or proposed at the federal level alone, not including SLTT requirements.[8] The compliance burden this patchwork imposes on covered entities is not merely administrative. When incident response teams are managing parallel reporting obligations to multiple federal agencies during an active incident, it degrades the quality of both the response and the reports. CIRCIA has a genuine opportunity to serve as the unifying framework that simplifies this landscape.

To achieve that goal, we urge CISA to adopt a reciprocity principle: any cyber incident report submitted to another federal agency pursuant to an applicable federal requirement should, by default, satisfy CIRCIA's reporting requirements for that incident. CISA should then proactively request supplemental information where necessary to fulfill CIRCIA's purposes, rather than requiring covered entities to file separate parallel reports.

We also reiterate our June 2024 recommendation that CISA publish clear, objective criteria for determining when another reporting requirement qualifies as "substantially similar" under CIRCIA's existing harmonization authority.[9] Without such criteria, covered entities cannot reliably assess whether a report filed under another framework satisfies their CIRCIA obligations, and the harmonization objective cannot be meaningfully achieved in practice.

Finally, we continue to support the proposed unified, web-based reporting interface, which will reduce administrative burden and standardize reporting across covered entities. We encourage CISA to ensure the interface itself is adequately secured.

* * *

HackerOne appreciates the opportunity to provide additional input on the CIRCIA rulemaking through this process. We believe that by refining the definition of "substantial cyber incident" to reflect actual impacts on critical infrastructure, clarifying the exclusion for independent good-faith security research, and adopting a genuine reciprocity approach to harmonization,

[7] 91 FR 6794, 6795.
[8] 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.
[9] 89 Fed. Reg. 23644, 23671.

CISA can finalize a rule that is effective, proportionate, and supportive of the security research ecosystem. HackerOne remains committed to working 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