hackerone

13 November 2025

VIA ELECTRONIC SUBMISSION

Re: Cyber Resilience Act (CRA) Delegated Regulation on Specifying the Terms and Conditions for Applying the Cybersecurity-Related Grounds in Relation to Delaying the Dissemination of Notifications

HackerOne submits the following comments in response to the European Commission's consultation on the Commission Delegated Regulation supplementing Regulation (EU) 2024/2847 of the European Parliament and of the Council by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications ("Delegated Act").[1] We appreciate the opportunity to provide comments on this important initiative.

By way of background, HackerOne is a global leader in offensive security solutions. Our HackerOne Platform combines AI with the ingenuity of the largest community of security researchers to find and fix security, privacy and AI vulnerabilities across the software development lifecycle. The platform offers bug bounty, vulnerability disclosure, pentesting, AI red teaming, and code security. We are trusted by industry leaders such as Amazon, Anthropic, Crypto.com, General Motors, GitHub, Goldman Sachs, Uber, and the U.S. Department of Defense.

As a leader in coordinated vulnerability disclosure (CVD) and vulnerability management, HackerOne supports the European Commission's efforts to enhance cybersecurity resilience and ensure that notification processes are both secure and effective. However, while the Delegated Act appropriately reflects several important considerations to justify the delay of reporting to CSIRTs, we believe there are opportunities to further strengthen these provisions.

Before detailing our recommendations, we would like to thank the European Commission for recognizing that situations in which a CSIRT becomes aware of a vulnerability through a CVD process require careful handling to avoid premature disclosure. Additionally, we appreciate the Commission's recognition that delaying disclosure may be warranted when the details of a vulnerability are sufficient to enable the creation of an exploit that could be abused by attackers.[2] We appreciate this recognition; however, as noted in previous comments on the Cyber Resilience

[1] European Commission, Delegated Regulation on Specifying the Terms and Conditions for Applying the Cybersecurity-Related Grounds in Relation to Delaying the Dissemination of Notifications, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14731-Cybersecurity-terms-conditions-for-delaying-the-notification-of-incidents-delegated-act-_en.

[2] Hacking Policy Council, Cyber Resilience Act - Vulnerability Reporting Obligations, https://cdn.prod.website-files.com/62713397a014368302d4ddf5/648c6cc44c0f10df3fdf47a5_CRA%20Vulnerability%20Disclosure%20Obligations%20-%20HPC%20-%20April%204%202023.pdf

Act, "mere knowledge of a vulnerability's existence in a feature of some product is sufficient for a skillful person to discover it for themselves."

HackerOne has emphasized that premature vulnerability disclosure can inadvertently increase systemic risk by exposing organizations to exploitation before appropriate mitigations or patches are in place. Disclosing vulnerabilities before they are remediated provides potential attackers with actionable intelligence, heightening the likelihood of exploitation, targeted attacks, or surveillance. Furthermore, centralizing unpatched vulnerability reports could unintentionally concentrate risk, making ENISA and CSIRTs more attractive and high-value targets for malicious actors.

First, we recommend amending the strict timeline in Article 3(a), which authorizes a delay in notification if the relevant preconditions are met and the notifying manufacturer also indicates that an effective "risk mitigation measure" (*i.e.*, a security update or user guidance) will be available within 72 hours. If the risk mitigation measure is not made available within that timeframe, the receiving CSIRT must proceed with the notification (unless one of the other criteria in Articles 3(b), 3(c) or 3(d) applies). Seventy-two hours is often insufficient to ensure the development, testing, and deployment of a secure patch. Research shows that the median time to resolve a vulnerability can be as long as 52 days, underscoring that effective remediation and fix validation for many vulnerabilities can realistically be measured in weeks, not days.[3] Even when a fix involves updating only a few lines of code, identifying the precise lines can be like looking for a needle in a haystack – requiring careful validation to avoid introducing new vulnerabilities or disrupting system functionality.[4] This provision should be amended to allow reasonable extensions to the 72-hour timeline. An extension should remain available as long as the manufacturer is actively working on remediation. Organizations should be provided with sufficient time to remediate a discovered vulnerability before being compelled to disclose it, ensuring that disclosure supports security rather than inadvertently undermining it.

Second, Article 4(b) of the Delegated Act permits a receiving CSIRT to delay notification if it has "sufficient reason to believe that the capabilities of the relevant CSIRT are inadequate." In addition to concerns arising from cybersecurity incidents or capability gaps, there are several other legitimate, cybersecurity-related reasons why one CSIRT may be reluctant to disclose a particular vulnerability to another. For example, a receiving CSIRT may fear that a relevant CSIRT could broadly publicize or insufficiently safeguard sensitive information, including from foreign adversaries, even if the CSIRT possesses the necessary technical expertise and capacity to manage it responsibly. We have emphasized that any rules governing the handling of vulnerability information should explicitly prohibit its offensive use.[5] Laws requiring disclosure of vulnerabilities to government agencies for purposes such as market access, consumer safety, or incident response should include clear restrictions preventing the use of disclosed vulnerabilities for intelligence, surveillance, or offensive operations. To address these concerns,

[3] *See e.g.,* Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties, *Journal of Cybersecurity*, Volume 7, Issue 1 (2021), https://doi.org/10.1093/cybsec/tyab007
[4] The Cost Savings of Fixing Security Flaws in Development, https://www.hackerone.com/blog/cost-savings-fixing-security-flaws
[5] How EU Lawmakers Can Make Mandatory Vulnerability Disclosure Responsible, https://www.helpnetsecurity.com/2023/08/21/vulnerability-disclosure/

HackerOne urges the Commission and ENISA to establish harmonized, EU-wide standards governing the use, dissemination, and retention of vulnerability information.

Finally, while the Delegated Regulation clarifies that ENISA's access to notifications cannot normally be delayed or restricted, we urge the Commission to expand the scope of these measures to explicitly include ENISA. As ENISA routinely handles sensitive vulnerability information, manufacturers should also have the ability to delay premature vulnerability reporting to the agency when justified by cybersecurity-related risks. Such delays should be permitted under the same conditions and justifications that apply to other CSIRTs, ensuring a consistent and risk-based approach to information sharing across the EU.

* * *

HackerOne appreciates the European Commission's continued leadership in advancing the European Union's cybersecurity framework through the Cyber Resilience Act and this Delegated Regulation. We commend the Commission for recognizing the importance of cybersecurity-related grounds for delaying dissemination to CSIRTs, particularly in cases where disclosure could enable the creation or exploitation of vulnerabilities. HackerOne stands ready to collaborate with the European Commission in the implementation of these measures.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne