hackerone

March 11, 2026

VIA ELECTRONIC SUBMISSION

Re: Digital Fitness Check – Testing the Cumulative Impact of the EU's Digital Rules

HackerOne submits the following comments in response to the European Commission's consultation on the Digital Fitness Check.[1]

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 like IKEA, Lufthansa, the Financial Times, Spotify, Beiersdorf, and Vodafone.

HackerOne actively contributes to EU digital policy discussions, providing input on key legislative files shaping the EU's digital rulebook, including the Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554), NIS 2 Directive (Directive (EU) 2022/2555), AI Act (Regulation (EU) 2024/1689), and Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847). Through this engagement, we have seen both the strengths of the EU's cybersecurity framework and areas where greater harmonization and clarity could support more effective implementation.

Ensuring Legal Certainty and Safe Harbor Protections for Good-Faith Security Research

Good-faith security research is fundamental to the safety and resilience of critical infrastructure, government networks, and connected devices. The public benefits when security weaknesses in software, hardware, and digital systems are identified and remediated before malicious actors can exploit them. Independent researchers acting responsibly have often discovered serious vulnerabilities and disclosed them appropriately, helping to prevent data breaches, service disruptions, financial losses, and consumer harm.

Despite these benefits, researchers conducting good-faith vulnerability testing can still face legal uncertainty when their findings are unwelcome or misunderstood. The risk of criminal charges, civil liability, contractual penalties, or reputational damage creates significant unpredictability.

[1] European Commission, *Digital Fitness Check – testing the cumulative impact of the EU's digital rules,* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/15554-Digital-fitness-check-testing-the-cumulative-impact-of-the-EUs-digital-rules_en.

Even if sanctions never materialize, the mere possibility can have a chilling effect on responsible research and disclosure.

HackerOne appreciates that the EU's digital regulatory framework increasingly acknowledges the value of security researchers and encourages Member States to address, to the extent possible, the challenges faced by vulnerability researchers. However, encouragement alone is insufficient. While a limited number of Member States – including Portugal, Malta, and Belgium – have introduced measures aimed at clarifying protections for security researchers, these approaches remain uneven in scope and legal certainty. The result is a fragmented landscape in which the protections available to a good-faith researcher may vary significantly depending on jurisdiction.

The absence of clear, harmonized safe harbor protections leaves good-faith researchers dependent on divergent national interpretations and discretionary enforcement practices. This fragmentation undermines legal certainty, creates inconsistent levels of protection across the internal market, and risks chilling legitimate research activity, particularly in a cross-border digital environment where vulnerabilities routinely affect multiple Member States simultaneously.

We believe that the Digital Fitness Check presents a timely opportunity to create a more coherent and harmonized approach to safe harbor protections for all Member States that would enhance legal clarity and reinforce the objectives of existing legislation.

* * *

HackerOne appreciates the opportunity to submit comments in response to this call for information. If we can be of further assistance, please contact the HackerOne Policy Team at policy-team@hackerone.com.

Respectfully,

Ilona Cohen
Chief Legal and Policy Officer,
HackerOne