April 13, 2026

Re: The Hacking Policy Council's Submission on the European Commission's Draft Cyber Resilience Act (CRA) Guidance

The Hacking Policy Council ("HPC) submits the following comments to the European Commission's consultation to provide guidance on how to apply the Cyber Resilience Act (CRA) in practice.[1] We appreciate the Commission's ongoing efforts to promote a consistent and effective cybersecurity framework across the European Union and welcome the opportunity to provide input aimed at supporting clear, workable expectations for entities placing digital products on the market.

As the Commission develops implementation guidance, it will be important to ensure that regulatory expectations align with established security practices and do not inadvertently limit the contributions of the independent research community. In particular, clarity and flexibility will be critical to ensuring that organizations can meet their obligations while maintaining effective channels for identifying and addressing vulnerabilities.

The HPC is a group of experts dedicated to creating a more favorable legal, policy, and business environment for good faith security research, penetration testing, independent repair for security, and vulnerability disclosure and management.[2] In this submission, HPC focuses on three areas: first, the importance of security testing as a foundational element of CRA compliance; second, the interpretation of reporting obligations under Article 14, particularly where vulnerabilities are identified through third-party reporting and coordinated vulnerability disclosure processes; and third, the practical application of vulnerability handling requirements in a manner that reflects real-world risk management and remediation workflows.

I. Scope and Security Testing (Paragraph 166)

HPC recognizes that, as reflected in Recital 11, the CRA does not intend to treat systems used for security testing, such as penetration testing, threat hunting, and red teaming, as products with digital elements within scope. This distinction is helpful in clarifying that such activities and supporting systems are not themselves subject to CRA product requirements. At the same time,

[1] European Commission, Draft Guidance on the Cyber Resilience Act, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959-Draft-Commission-guidance-on-the-Cyber-Resilience-Act_en.
[2] Hacking Policy Council, https://hackingpolicycouncil.org.

the guidance should more clearly reinforce that these activities remain essential to fulfilling the CRA's substantive cybersecurity obligations, including the requirement under Annex I to perform effective and regular security testing. In practice, adversarial and independent testing approaches are critical to identifying vulnerabilities that may not be detected through internal processes alone and to validating whether products meet the required level of security. Clarifying this relationship would help avoid any unintended interpretation that the exclusion of testing systems from scope diminishes the importance of testing itself.

II. Vulnerability Reporting (p. 193-200)

Regarding reporting obligations under Article 14, HPC recognizes the Commission's effort to provide greater clarity on when a manufacturer should be considered to have sufficient knowledge of a vulnerability or incident to trigger reporting requirements. In practice, many vulnerabilities are surfaced through external reports, including those submitted through coordinated vulnerability disclosure frameworks. These reports often require validation, contextual analysis, and technical confirmation before their significance can be fully understood. For this reason, it is important that the concept of "awareness" is interpreted in a manner that allows for reasonable assessment and verification, rather than being tied to the initial receipt of unconfirmed information. An approach that triggers obligations too early in the process may create unintended pressure on organizations to act on incomplete data and could discourage the maintenance of open reporting channels that are critical to effective vulnerability discovery. HPC therefore encourages the Commission to clarify that reporting obligations should be tied to validated understanding, while continuing to support coordinated vulnerability disclosure processes as a key mechanism for identifying and addressing vulnerabilities.

III. Vulnerability Handling (p. 201-207)

Finally, HPC supports the objective of improving supply chain security through the sharing of vulnerability remediation information with upstream component providers, as reflected in Article 13(6) and paragraph 205. Enabling fixes to be addressed at the component level can contribute to more comprehensive risk reduction across products that depend on shared technologies. At the same time, implementation guidance should reflect the practical complexities associated with this process. Preparing a remediation for upstream use, particularly in a format that is standardized, verifiable, and suitable for broader integration, often requires additional validation, cross-environment testing, and supporting documentation beyond what is necessary to remediate the issue within a single product. These additional steps can require significant time and resources. As a result, there may be instances where manufacturers must sequence their actions, prioritizing timely mitigation for affected users while concurrently preparing fixes for upstream coordination. Guidance that recognizes this reality would help ensure that supply chain remediation objectives are achieved without inadvertently slowing down immediate risk reduction efforts.

* * *

HPC appreciates the Commission's continued engagement in developing practical guidance to support effective implementation of the Cyber Resilience Act. As the CRA's implementation nears, it will be important that guidance reflects how vulnerabilities are identified, assessed, and remediated in real-world environments. HPC remains available to engage further with the Commission and other stakeholders as this work progresses.

Sincerely,

The Hacking Policy Council