hackerone

January 9, 2025

Konstantinos MOULINOS
Cybersecurity Expert
European Union Agency for Cybersecurity (ENISA)

Marianthi THEOCHARIDOU
Cybersecurity Expert
European Union Agency for Cybersecurity (ENISA)

VIA ELECTRONIC SUBMISSION

Re: Open Consultation on ENISA Draft Implementing Guidance on the European Commission's NIS 2 Implementing Act

Dear Mr. MOULINOS and Ms. THEOCHARIDOU,

HackerOne Inc. (HackerOne) submits the following comments in response to the European Union Agency for Cybersecurity's (ENISA) draft Implementing Guidance on NIS 2 Security Measures.[1] HackerOne appreciates the opportunity to provide input, and we commend ENISA for its work with European Union Member States and industry stakeholders to facilitate the clear and consistent implementation of the NIS 2 Directive.

HackerOne is the global leader in vulnerability elimination through continuous security testing. Its industry-leading HackerOne Platform combines AI with the expertise of the world's largest community of security researchers to deliver ongoing vulnerability discovery and management across the software development lifecycle. The platform offers bug bounty, vulnerability disclosure, pentesting, code audits, challenges, and AI red teaming.

Our comments center around the vulnerability management practices described in Section 6 of ENISA's Implementing Guidance, which reflects the European Commission's Implementing Regulation Annex.

Vulnerability Management

HackerOne strongly supports the vulnerability management practices described in the NIS 2 Implementing Regulation Annex under Section 6: *Security in Network and Information*

[1] European Union Agency for Cybersecurity (ENISA), *Implementing Guidance on Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures*, November 7, 2024, https://www.enisa.europa.eu/publications/implementation-guidance-on-nis-2-security-measures.

Systems Acquisition, Development and Maintenance (Article 21(2), Point (E), of Directive (EU) 2022/2555). We commend ENISA for clarifying these practices through its guidance, specifically on the following subsections:

Section 6.5: Security Testing – *"The relevant entities shall establish, implement and apply a policy and procedures for security testing."*[2] We support ENISA's draft Implementing Guidance to Section 6.5.2 – "Consider a range of security tests, e.g. vulnerability assessments, penetration testing, code review, ethical hacking, cyber-attack simulations or cyber response exercises etc."[3] HackerOne agrees that these practices are key parts of a holistic vulnerability management policy and implementing them will help many organizations improve their cybersecurity. However, ENISA should reference additional key testing methods that help organizations proactively identify and mitigate vulnerabilities. HackerOne encourages ENISA to add reference to the following practices in its Implementing Guidance:

- ***Bug Bounty Programs:*** Bug bounty programs (BBPs) incentive ethical hackers with monetary rewards to find vulnerabilities in an organization's system, providing an additional layer of security. BBPs are especially effective at uncovering vulnerabilities that automated scanners may miss. Unlike automated tools, BBPs leverage a broad network of security experts who are capable of simulating real-world attacks from the perspective of potential adversaries. We encourage ENISA to note that organizations should consider BBPs as a form of security testing to implement under Section 6.5.2.
- ***Red Teaming:*** Red teaming is a test where ethical hackers simulate real world threats, usually to accomplish a specific objective (e.g., exfiltrate data or disrupt operation). This is in contrast to penetration testing, wherein ethical hackers attempt to simply breach a system's security for the purpose of vulnerability identification. Red teaming, like bug bounty programs and penetration testing, takes advantage of the expertise of ethical hackers and external cybersecurity experts. We encourage ENISA to include red teaming in the list of tests organizations should consider under Section 6.5.2.

Section 6.10: Vulnerability Handling and Disclosure – *"The relevant entities shall obtain information about technical vulnerabilities in their network and information systems,*

---

[2] European Commission, *Annex Commission Implementing Regulation laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers*, Page 14, November 19, 2024, https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

[3] European Union Agency for Cybersecurity (ENISA), *Implementing Guidance on Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures*, Page 79, November 7, 2024, https://www.enisa.europa.eu/publications/implementation-guidance-on-nis-2-security-measures.

evaluate their exposure to such vulnerabilities, and take appropriate measures to manage the vulnerabilities."[4] HackerOne commends ENISA for its guidance on vulnerability handling and disclosure, especially Section 6.10.2, which urges covered entities to "identify a single point of contact and communication channels for network and information security related issues with suppliers and service providers."[5] To improve clarity, we believe ENISA should explicitly recommend the adoption of a formal Vulnerability Disclosure Policy (VDP) as part of a comprehensive vulnerability management strategy. A clear and well-defined VDP would provide a structured framework for receiving and responding to vulnerability reports from external sources, such as security researchers, vendors, and service providers. This would ensure that vulnerabilities are identified, evaluated, and remediated prior to reporting them to their designated CSIRTs.

However, under this same section, we advise against encouraging covered entities to "disclose not yet known vulnerabilities to their designated CSIRT" rather than directly to the affected organization. Under the NIS 2 directive, there is no obligation to disclose newly discovered vulnerabilities to CSIRTs prior to mitigation or exploitation. Best practices for vulnerability disclosure generally direct organizations to share unmitigated vulnerability information only on a need-to-know basis.[6] Unless circumstances require sharing information more broadly, such as prolonged lack of response from the affected organization, vulnerability reporters should minimize exposure of vulnerability information prior to mitigation.

Conclusion

HackerOne appreciates the opportunity to provide comments to this open consultation. As the conversation around NIS 2 implementation continues to evolve, we would welcome the opportunity to further serve as a resource and provide insights.

---

[4] European Commission, *Annex Commission Implementing Regulation laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers*, Page 16, November 19, 2024, https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks.

[5] European Union Agency for Cybersecurity (ENISA), *Implementing Guidance on Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures*, Page 93, November 7, 2024, https://www.enisa.europa.eu/publications/implementation-guidance-on-nis-2-security-measures.

[6] Hacking Policy Council, Position Statement: Requiring Vulnerability Disclosure to Governments, June 3, 2024,https://cdn.prod.website-files.com/62713397a014368302d4ddf5/648c6c0cb8458ee10cf2c094_HPC%20public%20statement%20on%20laws%20requiring%20vuln%20disclosure%20-%20June%202023.pdf

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne