hackerone

August 9, 2024

VIA ELECTRONIC SUBMISSION

Code of Practice for Software Vendors Call for Views
Cyber Resilience Team – 4/48
DSIT
100 Parliament Street
London
SW1A 2BQ

Re: Call for Views on the Code of Practice for Software Vendors

Dear Viscount Camrose,

HackerOne Inc. (HackerOne) submits the following comments in response to the Department for Science, Innovation & Technology's (DSIT) Call for views on the Code of Practice for Software Vendors.[1] HackerOne appreciates the opportunity to provide input, and we commend DSIT for its openness in working with industry stakeholders on this important issue.

HackerOne is the global leader in human-powered security, harnessing the creativity of the world's largest community of security researchers with cutting-edge AI to protect digital assets. The HackerOne Platform combines the expertise of our elite community and the most up-to-date vulnerability database to pinpoint critical security flaws across your attack surface. Our integrated solutions, including bug bounty, pentesting, code security audits, spot checks, and AI red teaming, ensure continuous vulnerability discovery and management throughout the software development lifecycle. HackerOne has helped find and fix vulnerabilities for sector leaders including Coinbase, General Motors, GitHub, Goldman Sachs, the Financial Times, Starling Bank, the U.S Department of Defense, and the UK Ministry of Defence.

Our comments centre around *Principle 3: Secure deployment and maintenance*, specifically as it relates to vulnerability management practices and safe harbours. In addition to our statement, we provide direct responses to select questions from DSIT's *Call for views survey questionnaire* in Appendix I.

Vulnerability Management

[1] Department for Science, Innovation & Technology (DSIT), *Call for views on the Code of Practice for Software Vendors*, 18 July 2024, https://www.gov.uk/government/calls-for-evidence/call-for-views-on-the-code-of-practice-for-software-vendors/call-for-views-on-the-code-of-practice-for-software-vendors#annex-c-call-for-views-survey-questionnaire.

HackerOne strongly supports Principle 3: Secure deployment and maintenance in the Code of Practice. In particular, we are encouraged by the inclusion of Vulnerability Disclosure Programs (VDPs) in provision 3.2: “Ensure the organisation implements and publishes an effective vulnerability disclosure process.” We believe that VDPs are key to building strong vulnerability management programs, which ultimately help raise the bar for cybersecurity across all sectors.

However, there are more vulnerability management practices beyond VDPs that software developers could implement to improve their cybersecurity. We encourage DSIT to include references to the following in Principle 3:

- ***Bug Bounty Programs:*** A program wherein a software developer offers a monetary reward to ethical hackers for successfully discovering and reporting a vulnerability or bug to them. Bug bounty programs allow companies to incentivize the ethical hacking community to continuously improve their systems’ security posture. Bug bounties can complement existing security controls by exposing vulnerabilities that automated scanners miss, since security researchers can emulate the attack vectors of a potential bad actor.
- ***Penetration Testing:*** A test where an ethical hacker attempts to breach a system's security for the purpose of vulnerability identification. Penetration testing, like bug bounty programs, takes advantage of the expertise of ethical hackers and external cybersecurity experts.
- ***Red Teaming:*** Similar to penetration testing, this is a test where ethical hackers simulate real world threats, usually to accomplish a specific objective. Red teaming, like bug bounty programs and penetration testing, takes advantage of the expertise of ethical hackers and external cybersecurity experts.

HackerOne also encourages DSIT to explicitly state that software producers may use third-party cybersecurity providers to create and maintain vulnerability management programs on their behalf. Software producers can leverage third-party expertise and existing tools that streamline the creation and maintenance of a robust vulnerability disclosure and management program and promote engagement with the ethical hacker community. To accomplish this, DSIT could include these descriptions in the technical controls of an existing principle - such as provision 3.2 - or create a “should” provision 3.6 dedicated to them.

Safe Harbours

Ethical hackers (also referred to as “good faith security researchers”) play an essential role in building a safer and more secure digital world. As such, those who ethically disclose vulnerabilities should do so without threat of legal action or regulatory sanction. HackerOne supports the inclusion provision 3.6, which encourages software producers to “make a public affirmation that the organisation would welcome security researchers to test software products and services provided by the organisation as part of its vulnerability disclosure process.”

However, we believe that DSIT should more explicitly recommend the creation of a "safe harbour," a provision where a company states that ethical hackers engaged in good faith security research and ethical disclosure are authorised to conduct such activity and will not be subject to legal action. Ethical hackers have reported that they are less likely to report vulnerabilities if there is uncertainty about such a safe harbour.[2] To ensure that software producers can experience the benefits of good faith security research, DSIT could include guidance on how to craft a "gold standard" safe harbour standard in a technical control for provision 3.6.[3] This guidance could encourage software producers to 1) apply safe harbour by default to all good faith security research ethically disclosed to an organisation; 2) seek mutual agreement with hackers on what constitutes good faith security research; and 3) not remove safe harbour retroactively. DSIT could also reference the UK Ministry of Defence's safe harbour provision as an example.[4]

Technical Controls

The technical controls listed in Chapter 5 lack sufficient specificity to be useful to software producers with limited cybersecurity experience. While we understand that DSIT likely will provide further details in implementation guidance, it is important to ensure sufficient information is included in the initial Code of Practice to enable software producers to operationalize its principles. Therefore, we urge DSIT to include references to additional cybersecurity best practices, such as bug bounty programs, red teaming, penetration testing, and third party cybersecurity services, in the technical controls.

Conclusion

HackerOne appreciates the opportunity to provide comments to this call for views. As the conversation around this topic continues to evolve, we would welcome the opportunity to further serve as a resource and provide insights on how to raise the standard for cybersecurity amongst software developers.

* * *

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne

---

[2] HackerOne, *Hacker-Powered Security Report 2022*, p. 10, https://www.hackerone.com/resources/i/1487910-2022-hacker-powered-security-report-q4fy23/0?.
[3] HackerOne, *Safe Harbor FAQ,* https://docs.hackerone.com/en/articles/8494502-safe-harbor-faq.
[4] Ministry of Defence, *Guidance: Report a vulnerability on an MOD system,* 8 December 2020, https://www.gov.uk/guidance/report-a-vulnerability-on-an-mod-system.