hackerone

March 24, 2025

VIA ELECTRONIC SUBMISSION
initiatives.dgp-asd-cyber@diplomatie.gouv.fr
pallmallprocess@fcdo.gov.uk

Re: Pall Mall Process Draft Code of Practice for States to Tackle the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities REV2

Dear Sir or Madam,

HackerOne submits the following comments in response to the Pall Mall Process Draft Code of Practice for States (rev2). We commend the UK and France for their leadership on this critical issue and for allowing stakeholders to contribute feedback.

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 Amazon, Anthropic, Crypto.com, General Motors, GitHub, Goldman Sachs, Uber, and the U.S. Department of Defense.

We support the Code's commitment to addressing the misuse of commercial cyber intrusion tools, but we believe there are key areas that could be enhanced. Below are our recommendations:

Section 2 – Voluntary Good Practice for States

Pillar 2 – Precision

We appreciate the expansion of provision 9.a.v., which "establishes clear policies on what constitutes legitimate use of CCICs in the context of cybersecurity (for example penetration testing, red teaming and coordinated vulnerability disclosure policies) and research for cybersecurity activities, aligned to existing protections or safeguards for cybersecurity researchers." However, we strongly recommend that bug bounty programs (BBPs) be explicitly recognized as a critical component of vulnerability testing.

By offering clear incentives for responsible vulnerability disclosure, BBPs help create a legitimate, ethical alternative that reduces the appeal of exploit markets and encourages researchers to report vulnerabilities to organizations in a controlled, structured environment.

Governments and organizations should view BBPs as an effective tool for strengthening cybersecurity while minimizing the risks posed by these illicit markets. By incentivizing BBPs, the cybersecurity ecosystem can empower researchers and vendors to work collaboratively to identify and resolve vulnerabilities before they can be exploited maliciously.

In addition, HackerOne supports provision 9.d.iii, which urges states to “raise awareness amongst cybersecurity professionals, including independent security researchers, of the implications of their work and the use of CCIC.” While many good faith security researchers are already aware of the implications of their work and the risks involved, HackerOne believes that awareness programs, guidelines, and best practices can be helpful to ensure that all cybersecurity professionals understand the broader consequences of their activities.

We also support 9.d.iv, which calls on states to “identify opportunities to coordinate to ensure efforts to establish best practices for professionals operating across the market for CCICs, including independent security researchers, are coherent internationally.” The global nature of cybersecurity threats necessitates international coordination and collaboration. As such, states should work together to establish common standards and best practices that can be followed by cybersecurity professionals worldwide.

Pillar 3 - Oversight

HackerOne remains concerned with provision 10.b.i, which encourages states to “explore controls for researchers contracting with Governments to ensure their work does not directly contribute to irresponsible activity across the market for CCICs.” We believe that imposing controls on researchers working with governments would be counterproductive. While preventing the misuse of cyber intrusion tools is important, restricting legitimate security research would inadvertently hinder efforts to strengthen cybersecurity, create a chilling effect, and delay timely responses to emerging threats.

Rather than imposing broad controls, we recommend that governments develop clear, comprehensive guidelines for good faith security researchers. These guidelines should delineate a framework for ethical conduct and best practices, detailing the scope of permissible activities, based on the systems involved, and expected good faith behavior, both for security researchers and organizations.

Pillar 4 – Transparency:

Finally, as mentioned in our previous comments, we appreciate the updated provision 11.a.ii, which calls on states to identify opportunities to better support and protect the commercial, civil society and independent cyber threat researcher ecosystem, including from intimidatory litigation.

While the intention of this provision is commendable, legal uncertainties around security research continue to pose significant barriers. Many researchers, even when acting in good faith, face the potential risk of legal consequences due to vague or outdated laws. Without clear legal distinctions between legitimate security research and malicious criminals, researchers may be deterred from contributing to the improvement of cybersecurity, thus hindering progress and innovation in the field. As a result, we believe this provision should be strengthened to explicitly urge states to adopt legal protections for security researchers.

* * *

HackerOne

HackerOne appreciates the opportunity to provide a response to this process. As the conversation around this topic continues to evolve, we welcome the opportunity to further serve as a resource and provide insights on promoting good faith security research while curbing the misuse of cyber intrusion capabilities.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne