HACKING POLICY COUNCIL

December 22, 2025

The Hacking Policy Council ("HPC") submits the following comments in response to the Pall Mall Process's Consultation on Good Practice for Industry.[1] We thank the UK and French governments in advancing global efforts to reduce the risks associated with commercial cyber intrusion capabilities (CCICs) and to promote responsible state and industry practices in this domain. 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. We respectfully offer the following recommendations and insights.

I. Recommendations of the Hacking Policy Council

As previously noted in our filings, HPC is skeptical that additional guidelines or new restrictions for industry, civil society, and independent researchers will produce benefits that justify the substantial compliance burdens and chilling effects they would impose. The private sector already operates under many outdated and overbroad computer access and use laws that often fail to adequately protect good-faith research. It must also navigate complex export-control regimes governing dual-use technologies, strict liability frameworks for inadvertent sanctions violations, and broad obligations under privacy and data-protection laws. Despite this challenging legal landscape, many commercial offensive security companies and practitioners, especially independent researchers, comply with these requirements and avoid knowingly contributing to activities that endanger human rights. Expanding restrictions on who conducts security work, and how they do it, would be aiming at the wrong target.[2]

The most significant risks associated with commercial cyber intrusion capabilities stem from the procurement and deployment decisions of state actors and a small subset of vendors whose business models rely on secrecy and the absence of meaningful oversight. Additional burdens on ethical practitioners would do little to curb misuse while simultaneously weakening the very ecosystem – responsible research, vulnerability discovery, penetration testing, and coordinated

[1] Pall Mall Process, Draft Code of Practice for Industry
[2] Hacking Policy Council Comments on Pall Mall Process Consultation on Good Practice Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities (CCICS), https://cdn.prod.website-files.com/660ab0cd271a25abeb800453/670fd0e07bbd452b76de046f_Hacking%20Policy%20Council%20-%20Pall%20Mall%20Process%20Comments%2020241014%20(1).pdf.

disclosure – that strengthens global cybersecurity and helps protect individuals from the harms the Pall Mall Process seeks to address.

For these reasons, the HPC urges that any guidance or recommendations emerging from this consultation be calibrated carefully. Efforts should support and reinforce beneficial security practices rather than hinder them, and should prioritize interventions targeted at the genuine drivers of irresponsible CCIC use.

II. Questionnaire Addressed to Commercial Cyber Intrusion Stakeholders

Standards and Requirements

1. *How would you describe your organisation, activity and interest in this market?*

HPC is an advocacy organization dedicated to create a coherent legal and policy environment that protects and encourages ethical hacking, coordinated vulnerability disclosure, penetration testing, and AI red teaming – activities that strengthen security, not undermine it. HPC's interest in this market arises from the direct impact that regulatory or policy changes in the commercial cyber intrusion space may have on legitimate security research and vulnerability management practices. Many of the challenges facing the cybersecurity ecosystem already stem from vague, outdated, and overly broad laws that fail to distinguish between malicious intrusion and authorized testing or security research. New legal obligations directed at "cyber intrusion capabilities" risk further entangling legitimate security work unless these distinctions are expressly recognized.

2. *What domestic laws or other requirements is your organisation required to adhere to when carrying out its activity?*

HPC members are subject to an extensive body of both U.S. and international legal and regulatory requirements that govern their cybersecurity, research, disclosure, and commercial activities. Because our membership includes global companies operating across numerous jurisdictions, it would be impractical to enumerate every potentially applicable statute, regulation, and legal obligation. However, all HPC members are established entities that maintain robust compliance programs and operate within the law.

In the United States, a significant governing statute members must comply with is the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, which defines unauthorized access and imposes both civil and criminal liability for misuse of computer systems. Importantly, the United States is one of the few jurisdictions that has formally acknowledged the distinction between malicious intrusion and legitimate security research. The Department of Justice (DOJ) issued a binding CFAA charging policy instructing federal prosecutors not to bring charges against individuals engaged in good-faith security research.[3] This policy explicitly recognizes that vulnerability research, penetration testing, and coordinated disclosure are essential to

[3] U.S. Dept. of Justice, Charging Policy - 9-48.000 Computer Fraud And Abuse Act, May 19, 2022, https://www.justice.gov/media/1223666/dl?inline.

strengthening security and should not be chilled by overly broad interpretations of the CFAA. We recommend that any government developing CCIC governance frameworks adopt a clear legal distinction between malicious activity and authorized security research, consistent with the DOJ's approach, and incorporate explicit protections for good-faith researchers. Other countries are looking to include these protections, especially as part of NIS2 transpositions as in Portugal or as updates to their own hacking laws as with the Computer Misuse Act in the United Kingdom.

3. *How do you ensure your organisation's activity aligns with the implementation of appropriate cyber or information security practices, including in terms of information access management? Which practices do you consider most important?*

HPC members maintain mature, well-established cybersecurity and information-governance programs that incorporate internationally recognized standards and best practices. As companies whose work directly involves identifying, triaging, and mitigating vulnerabilities across the global software ecosystem, our members apply stringent internal controls to ensure that security tools, testing methodologies, and sensitive information are handled responsibly and used exclusively for authorized purposes. These programs typically align with a wide range of frameworks, including ISO/IEC 27001 for information-security management, ISO/IEC 29147 and ISO/IEC 30111 for vulnerability disclosure and handling, the NIST Cybersecurity Framework, and the NIST Artificial Intelligence Risk Management Framework (AI RMF) for secure and trustworthy development, evaluation, and oversight. Many HPC members also adopt and promote best practices issued for the federal government, such as NIST SP 800-216 and the Internet of Things Cybersecurity Improvement Act of 2020 because these frameworks articulate clear expectations for coordinated vulnerability disclosure, device security, and software-assurance processes. Collectively, these frameworks reflect and inform the practices we consider the most important: vulnerability management, continuous monitoring, incident response, red-team operations, and threat modeling, each of which is essential to preventing malicious exploitation of vulnerabilities.

<u>Managing Risks</u>

7. *What due diligence measures are in place within your organisation to assess risks related to your activity (for example around diversion, re-selling or misuse) and what safeguards does your organisation put in place to manage them?*

Our members are constantly managing risk. Because of the nature of their work, identifying vulnerabilities, testing system defenses, and handling sensitive security information, they must continuously evaluate legal, operational, and human-rights risks associated with their activities. This includes assessing who is requesting testing or reporting assistance, how vulnerability information might be used, and whether any element of an engagement could be exploited in a manner inconsistent with lawful or authorized practices.

Additionally, we believe that the work we do with security researchers and through structured vulnerability-disclosure programs is itself a critical safeguard that reduces human-rights risks. By

identifying security weaknesses before malicious actors can exploit them, these activities strengthen protections for individuals, civil society organizations, and vulnerable communities. Responsible disclosure promotes transparency and accountability across the digital ecosystem, helping prevent intrusive surveillance, unlawful access, and other harms associated with the misuse of commercial cyber intrusion capabilities. Coordinated vulnerability disclosure also offers benefits through coordination with security researchers, allowing vetting against sanction lists and creating a legitimate market for security research and services. In many cases, independent research and coordinated vulnerability disclosure are the only mechanisms that alert the public and governments to the existence of security flaws that could threaten human rights.

Monitoring and Response

10. *What mechanisms does your organisation have in place to ensure secure reporting channels and protections for whistleblowers?*

HPC members operate some of the world's leading bug bounty platforms (BBPs) and vulnerability disclosure programs (VDPs), and therefore have substantial experience in maintaining secure reporting channels and protecting researchers who submit vulnerability information. Each member organization that maintains their own VDPs provide clear and secure pathways for reporting vulnerabilities, disclosure guidelines, and platform behavior standards. Additionally, our members implement legal safe-harbor provisions to protect good-faith security researchers from retaliation or legal exposure when they adhere to the organization's defined reporting procedures.

III. Questionnaire For Cyber Threat Intelligence Companies and Platform Providers

2. *What kind of public reporting or disclosures would help your organisation monitor the responsible use of commercial cyber intrusion capabilities?*

HPC believes that public reporting and disclosures related to commercial cyber intrusion capabilities should reinforce responsible state behavior without inadvertently increasing security risks. Premature or overly broad reporting requirements, such as those contemplated under the EU Cyber Resilience Act (CRA), which would mandate early-stage disclosure of actively exploited vulnerabilities, create substantial risk by compelling the release of sensitive information before a patch or mitigation is available. Forcing the disclosure of unmitigated vulnerabilities increases the likelihood that those same weaknesses will be exploited by malicious actors, including the very commercial cyber intrusion vendors and state entities whose misuse the Pall Mall Process seeks to curtail.

Instead, the most useful and appropriate public reporting mechanisms are those that increase government transparency regarding their own procurement, use, and handling of vulnerabilities and intrusion capabilities. Public disclosures that demonstrate governments are not stockpiling unpatched vulnerabilities for offensive use would meaningfully increase confidence in responsible state behavior and reduce incentives for exploit markets. Additionally, we

recommend that the Process encourage strict limitations on state purchase or use of zero-day vulnerabilities, coupled with a clear obligation for immediate vendor notification whenever a government becomes aware of a vulnerability that presents a meaningful risk of exploitation. These measures would also ensure that vulnerabilities are rapidly remediated rather than retained for offensive use.

Public reporting that strengthens the broader security ecosystem also plays an important role. Expanding the adoption of robust bug bounty programs and structured vulnerability disclosure policies (VDPs) across both public and private-sector organizations would encourage vulnerabilities to flow toward entities capable of remediation rather than toward exploit brokers or CCIC vendors. These programs provide threat-intelligence teams and platform providers with earlier insight into exploitation trends and enable faster detection of CCIC misuse.

The broader security industry already contributes substantial transparency that aligns with the objectives of the Pall Mall Process. Google's Project Zero and Threat Analysis Group, Microsoft's Threat Intelligence teams, Trend Micro's Zero Day Initiative and Pwn2Own program, and other research groups routinely publish detailed analyses of exploit chains, mercenary spyware operations, and sophisticated intrusion campaigns. These disclosures improve global situational awareness, highlight instances of CCIC misuse, and reduce the total number of exploitable vulnerabilities available to malicious actors. Industry-driven governance initiatives, such as Microsoft's Cybersecurity Tech Accord and Google's spyware-policy enforcement, further demonstrate voluntary commitments to responsible behavior and encourage higher standards across the private sector.

However, while industry transparency is valuable, the primary responsibility for preventing CCIC misuse rests with governments, as the dominant purchasers and deployers of commercial cyber intrusion tools. Governments must lead by example through greater transparency, responsible procurement practices, and meaningful accountability. Industry can support these efforts, but cannot substitute for them.

3. *If your organisation is a platform provider, what domestic laws or other requirements are you required to adhere to when managing vulnerabilities? What policies does your organisation implement to ensure a rapid and appropriate patching of disclosed vulnerabilities?*

See above.

IV. Questionnaire for Academia and Civil Society Organizations

1. *How would you describe your organisation and interest in this issue?*

HPC is not a civil society organization in the traditional sense, but our work intersects directly with the interests of civil society and independent security experts. Our interest is to ensure that efforts to regulate commercial cyber intrusion capabilities (CCICs) promote human rights, enhance transparency, and support, not hinder, the legitimate security practices that improve global resilience.

2. *How can CCIC activities be performed in a responsible way?*

CCIC activities can only be performed responsibly when they occur within strict legal, human-rights, and governance frameworks that clearly distinguish legitimate security practices from abusive or unlawful intrusion. Governments and organizations must also conduct rigorous due diligence on end users, assess human-rights risks, and ensure that CCIC tools are never deployed against journalists, human-rights defenders, political opponents, civil society groups, or other protected classes.

3. *What measures should be in place to improve CCIC standards, transparency and accountability?*

An essential measure for improving CCIC standards, transparency, and accountability is the protection and empowerment of the good-faith security research community. Ethical hackers, civil-society researchers, and independent analysts play a critical role in uncovering CCIC misuse, identifying systemic vulnerabilities, and exposing unlawful surveillance. For CCIC activities to be conducted responsibly, the legal environment must provide clear statutory protections and safe-harbor provisions that ensure researchers are not exposed to criminal, civil, or retaliatory action for responsible testing and disclosure. Without these protections, harmful vulnerabilities remain unreported and CCIC abuses become more difficult to detect. While we appreciate that the Code of Practice for States acknowledges the need to "identify opportunities to better support and protect the commercial, civil-society and independent cyber threat researcher ecosystem, including from intimidatory litigation," this commitment must be made far more explicit. The Industry Code of Conduct and any associated guidance should expressly include safe-harbor language that protects good-faith researchers from prosecution, civil claims, or contractual retaliation when acting within responsible disclosure processes.

6. *Would your organisation like to share additional recommendations?*

In previous iterations of the Pall Mall Process consultations, it was noted that stakeholders were "exploring opportunities to implement controls for researchers contracting with governments to ensure their work does not contribute to irresponsible activity across the market for CCICs."

HPC wants to reiterate that measures such as licensing requirements for security researchers would actively undermine the Pall Mall Process' objectives. Licensing frameworks introduce unnecessary barriers to entry that reduce the number and diversity of independent experts engaged in identifying vulnerabilities, monitoring CCIC misuse, and providing external accountability. These frameworks often involve bureaucratic, time-consuming, and opaque processes that many researchers are either unable or unwilling to navigate. The practical reality is that good-faith researchers frequently do not have the resources, institutional backing, or legal support required to undergo licensing regimes, and many will simply opt out of reporting or investigating vulnerabilities altogether rather than expose themselves to administrative hurdles or legal risk.

The consequences of these requirements are significant. Licensing frameworks suppress good-faith research, deter legitimate vulnerability reporting, and diminish the independent scrutiny required to detect unlawful or irresponsible CCIC activity. By reducing the pool of researchers willing or able to participate, such measures leave more vulnerabilities undiscovered and make CCIC misuse more difficult to identify. This outcome is directly contrary to the objectives of the Pall Mall Process and would weaken the very practices that strengthen cybersecurity and protect human rights.

V. Questionnaire for States

2. *What systems and procedures does your government have in place to respond to reports of suspected irresponsible activity by organisations involved in the cyber intrusion marketplace?*

The United States has maintained Executive Order 14093, "Commercial Spyware that Poses Risks to National Security," which created a formal mechanism for identifying, reviewing, and prohibiting engagement with commercial spyware vendors associated with human-rights abuses or other irresponsible activity. Under this order, U.S. agencies are barred from procuring or operationally using any commercial spyware that has been implicated in unlawful surveillance; used to target activists, journalists, academics, dissidents, political actors, or marginalized groups; or otherwise presents a significant risk of facilitating human-rights violations or undermining U.S. national-security interests. The Executive Order also requires interagency vetting and ongoing monitoring of vendors, including assessments of misuse, diversion, and human-rights impacts. When credible reports of irresponsible behavior arise, U.S. agencies are obligated to evaluate those reports and, where appropriate, suspend or terminate relationships with the vendor.

Beyond the Executive Order, the United States has taken additional steps to respond to irresponsible activity in the CCIC marketplace. The Department of Commerce has placed several surveillance-technology firms on the Entity List, restricting their access to U.S. components and technology. The Department of State has imposed visa restrictions on individuals who misused, or financially benefited from the misuse of, commercial spyware, including family members of such individuals.

* * *

Thank you for the opportunity to provide input to the consultation. If we can be of additional assistance, please contact Heather West at hewest@venable.com