HACKING POLICY COUNCIL

Comments on Pall Mall Process Consultation on Industry Guidelines to Tackle the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities

The Hacking Policy Council (HPC) appreciates the opportunity to provide comments in response to the Pall Mall Process consultation on the *Industry Guidelines to Tackle the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities (CCICs).* We commend the governments of the United Kingdom and France for their continued leadership in advancing the Pall Mall Process and bringing together governments, industry, academia, and civil society to promote the responsible development, transfer, and use of commercial cyber intrusion capabilities.

The HPC supports efforts to reduce the risks associated with the irresponsible use and proliferation of CCICs while preserving the legitimate security activities that strengthen cyber resilience. As a coalition 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 believe the proposed Industry Guidelines provide a strong foundation but would benefit from greater clarity and additional guidance to ensure they effectively address irresponsible uses of CCICs without inadvertently restricting legitimate defensive cybersecurity activities.

We respectfully offer the following recommendations to strengthen the proposed Industry Guidelines.

I. Section 1: Preface

As developers of increasingly capable AI systems, frontier AI companies are becoming key stakeholders in the cybersecurity ecosystem. Their models have the potential to both introduce new cyber risks and significantly strengthen cyber defenses. The current draft states that "the most advanced AI frontier models may provide high-end capabilities and lower the barrier of access to intrusion capabilities." While this appropriately recognizes the potential for misuse, it reflects only one aspect of AI's impact on cybersecurity.

Advanced AI models are also transforming legitimate defensive cybersecurity by enabling vulnerability research, secure code review, AI red teaming, malware analysis, vulnerability management, incident response, and software assurance. Because many commercial cyber intrusion capabilities—including spyware—ultimately depend on the discovery and exploitation of vulnerabilities, AI is increasingly shaping both the development of these capabilities and the ability to defend against them. The Industry Guidelines should recognize this dual role.

Although the Industry Guidelines do not apply directly to frontier AI companies, HPC believes they should be active participants in the Pall Mall Process. It is difficult to have a meaningful conversation about the future governance of commercial cyber intrusion capabilities without including the organizations developing AI models that are increasingly capable of discovering vulnerabilities and influencing both offensive and defensive cybersecurity. Engaging frontier AI companies alongside governments, industry, academia, civil society, and the security research community will help ensure that future iterations of the Guidelines remain technically informed, adaptable, and effective.

II. Section 3: Definitions

Proposed Definition of Vulnerability Research (Section 3 12.d.i.)

> *"Vulnerability research is activity that identifies and analyses potential weaknesses or flaws in computer systems and software that could be exploited to compromise systems or data. Legitimate vulnerability research, conducted with appropriate authorisation, can support cyber security. Examples of vulnerability research for this purpose include security testing and bug bounty programmes."*

HPC recommends revising the proposed definition of vulnerability research above to better reflect the breadth of legitimate defensive cybersecurity activities and to avoid unintentionally excluding good-faith research conducted outside formal authorization.

Many important vulnerabilities are discovered by independent researchers who are not engaged by, or granted prior authorization from, a technology provider. These researchers may inspect publicly accessible services, reverse engineer products to identify security weaknesses, and responsibly report vulnerabilities through coordinated vulnerability disclosure processes. Limiting legitimate vulnerability research to activities conducted with "appropriate authorisation" risks excluding these well-established cybersecurity practices.

Rather than defining legitimate vulnerability research by reference to prior authorization, HPC recommends that the Guidelines instead emphasize research conducted ethically, in good faith, and consistent with responsible vulnerability disclosure practices. This approach better reflects the important role that independent security research plays in identifying vulnerabilities before they can be exploited, strengthening software security, and reducing opportunities for the irresponsible use of commercial cyber intrusion capabilities.

To define responsible or good faith vulnerability research in Section 3, HPC recommends alignment with the terminology as defined in U.S. law:

"Good faith security research" means accessing a computer for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the

class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services." 37 CFR 201.40(b)(16).[1]

This definition excludes security research conducted for the purpose of selling vulnerability information to commercial spyware vendors or government agencies for cyber intrusion purposes. While such activity may be called "security research," it is neither in good faith nor for the purpose of promoting the security of the software or its users. HPC urges Pall Mall stakeholders to leverage this definition.

III. Section 4: Guidelines

Regulatory Compliance and Standards

Consistent with HPC's previous comments to the Pall Mall Process, we support the Guidelines' recognition of internationally accepted cybersecurity standards, including ISO/IEC 29147 and ISO/IEC 30111. These standards establish internationally recognized best practices for coordinated vulnerability disclosure and vulnerability handling, enabling organizations to receive, assess, coordinate, remediate, and communicate vulnerabilities in a consistent, transparent, and responsible manner.

HPC strongly encourages organizations to adopt and implement these standards as part of their cybersecurity governance and vulnerability management programs. Effective vulnerability disclosure and handling processes reduce the availability of unaddressed vulnerabilities that may otherwise be exploited by commercial cyber intrusion capabilities, including spyware, while strengthening trust between technology providers and the security research community. More broadly, implementing these standards supports responsible vulnerability management, improves software security and resilience, and advances the Pall Mall Process's objective of reducing the irresponsible use and proliferation of commercial cyber intrusion capabilities.

IV. Due Diligence

HPC supports the Guidelines' emphasis on risk-based due diligence for commercial actors engaged in the development, purchase, sale, transfer, or operation of commercial cyber intrusion capabilities. However, the Guidelines should make clear that these due diligence requirements are directed at commercial actors and should not extend to independent security researchers engaged in good-faith vulnerability research.

Independent researchers play a distinct role in the cybersecurity ecosystem by identifying vulnerabilities, reporting security weaknesses, and providing independent scrutiny of technologies and their misuse. Subjecting these researchers to commercial due diligence or vetting requirements could discourage legitimate research and vulnerability disclosure. Instead, governments and industry should promote clear best practices for good-faith security research,

[1] *See also* 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.

including expectations for responsible conduct and coordinated vulnerability disclosure, without making participation in such practices a prerequisite for conducting legitimate research.

V. Risk Management

HPC recognizes the value in implementing risk management approaches as important safeguards for commercial cyber intrusion companies. However, we strongly encourage this to also be delineated from security researchers.

In particular, Section 16.a.iv recommends vetting individuals provided with oversight of entire vulnerability chains, while Section 16.c.iii recommends establishing contractual rules authorizing employees' vulnerability research and exploit development outside of their work for the company. These measures may be appropriate as internal controls for commercial cyber intrusion companies seeking to manage access to sensitive vulnerabilities and capabilities. However, the Guidelines should make clear that they are not intended to establish a broader expectation that legitimate vulnerability research requires vetting, institutional authorization, licensing, registration, or other forms of prior approval.

HPC is particularly concerned that, absent this distinction, the combination of vetting and contractual authorization could be interpreted as endorsing a de facto licensing or permission regime for security research. HPC has consistently cautioned against approaches that discourage independent security research. Conditioning legitimate research on prior approval can create unnecessary barriers to entry and reduce the number and diversity of researchers identifying vulnerabilities, monitoring the misuse of commercial cyber intrusion capabilities, and providing independent accountability. Independent researchers, academics, and participants in coordinated vulnerability disclosure and bug bounty programs may not have an employment relationship, institutional sponsor, or other entity from which to obtain such approval. Faced with uncertainty about whether their research is permitted or additional administrative and legal burdens, some researchers may choose not to investigate or report vulnerabilities at all.

The consequences extend beyond individual researchers. Discouraging good-faith security research reduces independent scrutiny, weakens coordinated vulnerability disclosure, and leaves vulnerabilities undiscovered or unreported for longer periods of time. This can increase opportunities for those vulnerabilities to be exploited by malicious actors, including through commercial spyware. Such an outcome would run counter to the objectives of the Pall Mall Process by constraining activities that help identify irresponsible CCIC activity, improve cybersecurity, strengthen cyber resilience, and provide independent accountability.

HPC therefore recommends clarifying that the vetting and contractual requirements contemplated in Sections 16.a.iv and 16.c.iii are internal risk management measures for commercial cyber intrusion companies and their personnel. They should not be interpreted as establishing broader licensing, registration, authorization, vetting, or prior-approval requirements for independent researchers engaged in good-faith defensive cybersecurity activities.

VI. Monitoring and Oversight

HPC supports Section 17.c's recommendation that companies establish accessible processes for reporting irresponsible activity. These mechanisms should complement effective vulnerability disclosure and handling processes consistent with ISO/IEC 29147 and ISO/IEC 30111 and enable researchers to report vulnerabilities or evidence of misuse without unnecessary legal or procedural barriers. Clear and accessible reporting channels can strengthen independent oversight by enabling researchers and other external parties to identify and report irresponsible activity. Such mechanisms should encourage, rather than deter, good-faith research and reporting that can help detect misuse of CCICs and strengthen cybersecurity.

* * *

HPC supports the Pall Mall Process's objective of reducing the proliferation and irresponsible use of commercial cyber intrusion capabilities. To achieve that objective effectively, the Guidelines should expressly preserve and encourage good-faith security research, penetration testing, red teaming, coordinated vulnerability disclosure, and bug bounty programs, and should make clear that internal risk-management controls for commercial cyber intrusion companies do not create broader licensing, registration, vetting, or prior-authorization requirements for independent researchers. These distinctions are essential to ensuring that the Pall Mall Process strengthens, rather than inadvertently constrains, the cybersecurity ecosystem on which governments, companies, and users rely.