HACKING POLICY COUNCIL

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

September 25, 2026

The Hacking Policy Council (HPC) appreciates the opportunity to provide additional feedback on the revised Pall Mall Process Industry Guidelines. We thank the United Kingdom and France for considering stakeholder feedback and for making several changes as the Guidelines develop.

HPC welcomes the removal of language suggesting that legitimate vulnerability research depends on "appropriate authorization," an issue HPC specifically raised in its prior comments. HPC also supports the draft's recognition that good-faith security research is distinct from malicious or irresponsible activity, its clearer distinction between vulnerability research conducted in support of operational commercial cyber intrusion capabilities (CCICs) and activities conducted in support of vulnerability disclosure; its recognition of the important role played by independent researchers; and its retention of language encouraging Coordinated Vulnerability Disclosure (CVD) processes and publicly accessible Vulnerability Disclosure Programs (VDPs).

These changes address several concerns raised in HPC's prior comments. However, some provisions remain ambiguous or only partially resolve those concerns. To provide additional clarity, HPC offers the following recommendations on the revised Guidelines.

1. Part 2: Foundational Principles - Vulnerabilities Equities Processes (VEPs)

Paragraph 9: *Relevant norms include 13(c) that States should not knowingly allow their territory to be used for internationally wrongful acts using Information Communication Technology (ICT), norm 13(i) that States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and norm 13(j) that States should encourage responsible reporting of ICT vulnerabilities. This could be through initiatives such as structured state-level Vulnerabilities Equities Processes (VEPs), with reassurance that security research outcomes for government use will not be disclosed.*

Recommended Amendment:

Relevant norms include 13(c) that States should not knowingly allow their territory to be used for internationally wrongful acts using Information Communication Technology (ICT), norm 13(i) that States should seek to prevent the proliferation of malicious ICT tools and techniques and the

use of harmful hidden functions; and norm 13(j) that States should encourage responsible reporting of ICT vulnerabilities. This could be through initiatives such as structured state-level Vulnerabilities Equities Processes (VEPs), ~~with reassurance that security research outcomes for government use will not be disclosed~~ with appropriate safeguards to ensure that security research outcomes provided for government use are protected from unauthorized disclosure, and with a defined process for evaluating whether other vulnerabilities known to the government should be disclosed for remediation or retained for government use.

Comment:

HPC supports the inclusion of structured state-level VEPs but recommends additional clarification regarding their purpose and implementation. In particular, the Guidelines should:

- Protect security researchers and their research. Researchers providing sensitive security research for government use should have confidence that their work will be protected from unauthorized disclosure. Security research may contain sensitive technical information, including vulnerability details, proof-of-concept code, exploit techniques, or research methods, that could create security risks if disclosed without appropriate safeguards. Unauthorized disclosure could also discourage researchers from sharing valuable information with governments in the future. Clear safeguards governing how governments receive, handle, and protect this information are therefore important to maintaining trust between governments and the security research community.

- Treat protection of research and disclosure of vulnerabilities as separate decisions. Protecting security research provided to the government is separate from determining what the government should do with a vulnerability of which it becomes aware. For those vulnerabilities, a VEP should provide a defined process for deciding whether the vulnerability should be disclosed so that it can be remediated or retained for government use. That process should consider both the government's interest in retention and the cybersecurity risks associated with leaving the vulnerability unaddressed.

- Account for how AI is changing vulnerability discovery. Traditional VEPs generally contemplate evaluating vulnerabilities individually to determine whether disclosure or retention is appropriate. AI may complicate that model by increasing both the volume of vulnerabilities discovered and the speed at which they can be identified. It may also increase the likelihood that a vulnerability retained by one government will be independently discovered by another actor. If the Pall Mall Process recommends the use of VEPs, it should recognize these changing dynamics and ensure that decisions about vulnerability retention account for the increased likelihood of independent discovery and exploitation.

2. Part 2: Foundational Principles - Security Researchers

Paragraph 12.b: *Civil society and other private actors that monitor the cyber intrusion market, such as independent researchers, cyber threat intelligence and technology companies, play a*

critical role in detecting, identifying and exposing irresponsible behaviour, as well as disclosing vulnerabilities and enabling access to redress for victims. We encourage greater cooperation between States, the cyber intrusion industry, and these monitoring entities, in accordance with national regulations, to address irresponsible CCIC use. The cyber intrusion industry should not use forms of legal intimidation to prevent such actors from performing these functions.

Comment:

HPC welcomes the revised language expressly recognizing the important role independent researchers play in detecting and exposing irresponsible CCIC activity as well as disclosing vulnerabilities. This addition is consistent with HPC's prior Pall Mall comments emphasizing the importance of protecting legitimate security research and with HPC's broader efforts to reduce barriers that can discourage good-faith research and vulnerability disclosure.

HPC particularly appreciates the inclusion of language stating that the cyber intrusion industry should not use legal intimidation to prevent independent researchers from performing these functions and strongly supports retaining this protection in the final Guidelines. Legal threats can discourage researchers from investigating and reporting vulnerabilities or exposing evidence of irresponsible CCIC activity, reducing the independent scrutiny and accountability that the Guidelines themselves seek to encourage.

3. Part 3: Definitions - Vulnerability Research for Exploit Development (VRED)

Paragraph 14.a.ii: *Vulnerability research for exploit development (VRED) purposes: Services or deliverables, including vulnerability information, proof-of-concept exploit code, and exploit chains – when developed or supplied for incorporation into, or in operational support of, capabilities described in paragraph 14.a. This definition does not include activities conducted under and in support of vulnerability disclosure schemes.*

Recommended Amendment:

Vulnerability research for exploit development (VRED) purposes: Services or deliverables, including vulnerability information, proof-of-concept exploit code, and exploit chains – when developed or supplied for incorporation into, or in operational support of, capabilities described in paragraph 14.a. This definition does not include ~~activities conducted under and in support of vulnerability disclosure schemes~~ good-faith security research, penetration testing, red teaming, independent repair for security, coordinated vulnerability disclosure, or bug bounty activities.

Comment:

HPC welcomes the revised definition's clearer distinction between vulnerability research conducted in support of operational CCICs and activities conducted in support of vulnerability disclosure. In particular, HPC supports the addition of language expressly excluding activities conducted under and in support of vulnerability disclosure schemes. This is an important improvement and is consistent with HPC's prior comments emphasizing that legitimate

vulnerability research and disclosure should not be treated as part of the commercial cyber intrusion market.

The exclusion, however, remains narrower than the range of legitimate security research HPC sought to protect. Good-faith vulnerability research does not always occur under a formal vulnerability disclosure scheme. This distinction is particularly important because the revised Guidelines appropriately remove the previous language suggesting that legitimate vulnerability research must be conducted with "appropriate authorization." Limiting the exclusion to activities conducted under a vulnerability disclosure scheme could unintentionally reintroduce a similar limitation by tying protection for legitimate research to participation in a formal process.

Additionally, HPC appreciates the addition of footnote 3, which expressly recognizes that good-faith research is distinct from activities intended for malicious or irresponsible use. This clarification reinforces the important distinction between legitimate security research and activity undertaken in support of irresponsible CCIC use. HPC strongly supports retaining this language in the final Guidelines.

4. Part 4: Guidelines - Due Diligence

Paragraph 17: *Due Diligence – A continuous, embedded process that assesses the activities undertaken by the cyber intrusion industry in relation to activities that may result in human rights abuses. This includes verification that the activities of staff and contractors, customers and supply/value chain partners do not represent irresponsible use.*

Recommended Amendment:

For avoidance of doubt, the due diligence requirements in this Section do not apply to independent researchers engaged in good-faith security research. Nothing in this Section should be interpreted as establishing licensing, registration, vetting, or prior-approval requirements for independent researchers engaged in good-faith security research.

Comment:

HPC supports risk-based due diligence for actors participating in the commercial CCIC ecosystem. HPC previously recommended, however, that these requirements be clearly distinguished from independent researchers engaged in good-faith vulnerability research. The revised draft does not yet expressly provide that clarification.

Independent researchers occupy a different role from the commercial actors and counterparties contemplated by the due diligence framework. A researcher may interact with a company solely to report a vulnerability, participate in CVD, submit a finding through a bug bounty program, or provide information concerning suspected misuse. Such interaction should not transform the researcher into a supplier, contractor, business partner, or other commercial counterparty subject to the company's due diligence requirements.

HPC therefore recommends expressly carving independent good-faith researchers out of the commercial due diligence framework. This distinction should also be reflected in the specific risk assessment and vetting requirements in paragraph 17.d to ensure that the Guidelines consistently distinguish independent good-faith researchers from the commercial actors and personnel subject to due diligence.

5. Part 4: Guidelines – Risk Management: Employee Vulnerability Research and Exploit Development

Paragraph 18.c.iii: *Rules prohibiting or restricting activity involving vulnerability research and exploit development outside of their work for the company without prior authorisation or agreement of the employer.*

Recommended Amendment:

~~*Rules prohibiting or restricting activity involving vulnerability research and exploit development outside of their work for the company without prior authorisation or agreement of the employer.*~~

Rules prohibiting the unauthorized use, disclosure, transfer, or sale outside the scope of employment of proprietary CCIC capabilities, confidential vulnerability information, non-public exploit material, operational infrastructure, or other sensitive information or capabilities obtained through employment. This provision does not apply to independent researchers engaged in good-faith security research or establish a broader expectation that vulnerability research requires employer or institutional authorization.

Comment:

HPC supports appropriate internal controls for commercial cyber intrusion companies. Companies may reasonably restrict employees from using, disclosing, transferring, or selling proprietary CCIC capabilities, confidential vulnerability information, non-public exploit material, or other sensitive information obtained through their employment. Those controls, however, should be directed at the protection and misuse of company information and capabilities—not at vulnerability research itself.

HPC has consistently cautioned against approaches that condition legitimate security research on institutional authorization, licensing, registration, vetting, or other forms of prior approval. Such requirements can create unnecessary barriers to entry and discourage independent security research. Conditioning legitimate research on such approval could therefore exclude or deter precisely the researchers whose work helps identify vulnerabilities and provides independent scrutiny of the cybersecurity ecosystem.

These restrictions can also have broader cybersecurity consequences. Researchers faced with uncertainty about whether their work is permitted, or with additional administrative or legal burdens, may choose not to investigate or report vulnerabilities. This can reduce the number and diversity of researchers identifying security weaknesses, weaken coordinated vulnerability disclosure, and leave vulnerabilities undiscovered or unreported for longer periods of time. In

turn, those vulnerabilities may remain available for exploitation by malicious actors, including through commercial cyber intrusion capabilities.

6. Part 4: Guidelines – Risk Management: Coordinated Vulnerability Disclosure and Vulnerability Disclosure Programs

Paragraph 18.g: *Consider establishing and maintaining mechanisms enabling the secure reporting, assessment, prioritisation and remediation of vulnerabilities. Where appropriate, organisations should implement Coordinated Vulnerability Disclosure processes and publicly accessible Vulnerability Disclosure Programmes consistent with internationally recognised standards.*

Recommended Amendment:

Consider establishing and maintaining mechanisms enabling the secure reporting, assessment, prioritisation and remediation of vulnerabilities. Where appropriate, organisations should implement Coordinated Vulnerability Disclosure processes and publicly accessible Vulnerability Disclosure Programmes consistent with internationally recognised standards, including ISO/IEC 29147 and ISO/IEC 30111.

Comment:

HPC strongly supports the retention of paragraph 18.g and its express recognition of CVD processes and publicly accessible VDPs. HPC recommends adding ISO/IEC 29147 and ISO/IEC 30111, which were referenced in the prior draft and specifically supported in HPC's prior comments. These internationally recognized standards provide established guidance for vulnerability disclosure and handling and would give organizations greater clarity in implementing this provision.

* * *

HPC appreciates the progress reflected in the revised Industry Guidelines. The revisions better recognize the important role of good-faith security research, independent researchers, coordinated vulnerability disclosure, and other defensive cybersecurity activities in strengthening cyber resilience.

HPC's remaining recommendations are intended to ensure that these distinctions are reflected consistently throughout the final Guidelines. In particular, internal controls designed for actors participating in the commercial CCIC ecosystem should remain appropriately distinct from good-faith security research conducted independently of those activities.

As the Guidelines are finalized, HPC encourages similar clarity wherever researchers or research-related activities are referenced in connection with due diligence, vetting, monitoring, or oversight. Those provisions should be applied in a manner that preserves the distinction between researchers participating in covered CCIC activities and independent researchers engaged in legitimate security research and vulnerability disclosure.

Maintaining this distinction will help ensure that measures intended to address irresponsible CCIC activity do not inadvertently discourage the independent research and vulnerability disclosure that contribute to stronger cybersecurity and help identify potential misuse. Thank you again for the opportunity to provide comments. We appreciate the continued engagement and look forward to the next round of negotiations.