hackerone

29 August 2025

The Hon Tony Burke MP
Minister for Home Affairs
Minister for Cyber Security

VIA ELECTRONIC SUBMISSION

Re: Submission to Horizon 2 Consultation – HackerOne Response

Dear Minister Burke,

HackerOne, Inc. (HackerOne) submits the following comments in response to the Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy Policy Discussion Paper. HackerOne appreciates the opportunity to provide input.

By way of background, 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.

Mitigating vulnerabilities before they are exploited is far more cost-effective than recovering from an incident. HackerOne data shows that for every USD$1 invested in a vulnerability disclosure program or bug bounty program, organisations typically avoid around USD$20 in potential incident costs.

The empirical evidence and policy justification go beyond individual organisational savings:

- Macro impact: Cyber incidents cost the Australian economy an estimated AU$33 billion annually (ASD). Scaled adoption of VDPs would reduce this burden nationally by preventing breaches before they occur.

- National security: Unreported vulnerabilities present a persistent attack surface for adversaries, particularly in critical infrastructure. Embedding VDPs into the SOCI Act's Enhanced Cyber Security Obligations would strengthen sovereign resilience. Additionally, aligning with Australia's AUKUS partners—both of whom have institutionalised disclosure and bug bounty programs in their defence portfolios would

enhance strategic interoperability, reinforce shared cyber norms, and ensure that Australia can participate in joint threat reduction efforts with trusted partners.

- Industry competitiveness: Widespread adoption of VDPs across the Australian industry would position Australian firms to meet international compliance norms such as the EU's NIS2 Directive and expanding U.S. coordinated vulnerability disclosure standards, improving trust and market credibility while lowering assurance costs.

Australia has an opportunity to align with best practices emerging from international partners by creating a National Vulnerability Disclosure Framework that provides legal certainty, economic incentives, and scalable infrastructure to support secure reporting and triage.

Question 31: How could government better incentivise businesses to adopt vulnerability disclosure policies?

The Australian Government is uniquely positioned to catalyse national adoption of VDPs through a combination of legal reform, economic incentives, public-sector example-setting, and sustained engagement with the research and business communities. These efforts would not only enhance national cyber resilience but also align Australian industry with emerging global norms, such as those embedded in the EU's NIS2 Directive. This would help alleviate any remaining private sector hesitancy to adopt VDPs, whether due to legal uncertainty, lack of awareness, or perceived operational or reputational risks.

Public sector example-setting is critical. While Australian Government agencies are already required to maintain VDPs under the Protective Security Policy Framework (PSPF), increased transparency and promotion of these programs would encourage private sector adoption. Centralised resources, including templates, reporting tools, and triage support could help reduce friction for new entrants. The Australian Government can also lead by example by introducing bug bounty programs for key departments, such as the Department of Defence, bringing national practice in line with the respective defence ministries of its AUKUS partners, the United States Department of Defense and the United Kingdom Ministry of Defence. Both countries have run successful bug bounty initiatives that have uncovered numerous critical vulnerabilities in government systems. For example, the U.S. Department of Defense's 'Hack the Pentagon' and subsequent incentivized programs have led to the identification and remediation of over 7,000 vulnerabilities across military platforms to date, while the UK's Ministry of Defence reported significant security improvements through similar crowdsourced security testing efforts.

The government could also mandate or strongly encourage the adoption of VDPs for critical infrastructure operators under the Security of Critical Infrastructure (SOCI) Act. This could begin with entities designated as Systems of National Significance (SoNS) having VDP expectations applied within the Enhanced Cyber Security Obligations (ECSO). SOCI ECSO rules could prescribe that vulnerability assessments include externally facing VDPs with defined features such as scope, safe harbour terms, reporting channels, triage practices, and disclosure policies. Assessment reports could further describe how submissions are managed, response times, and remediation outcomes.

International experience shows that governments can successfully accelerate VDP adoption by clarifying the benefits, offering guidance, and addressing legal ambiguity. The Australia Government, led by the Department of Home Affairs and the Australian Cyber Security Centre, should ensure that these business cases are widely understood, with supporting materials and technical assistance provided to industry partners.

Question 32: Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

Yes. Australia urgently needs a nationally consistent VDP framework to empower security researchers to report vulnerabilities safely, legally, and in a structured manner. Without clear legal protections and policy guidance, many researchers currently operate in a grey zone—deterred from reporting issues due to the risk of criminal or civil liability under outdated computer crime laws. This not only chills valuable security research but weakens Australia's broader cyber defence posture.

Under current law, researchers risk prosecution under the Criminal Code Act 1995 (Cth) and state-based offences for unauthorised access, even where no harm is caused and the researcher acts in good faith. There is no statutory exemption or safe harbour, and whistleblower laws do not clearly apply. By contrast, international best practice is moving toward formal legal protections. Belgium, for instance, has passed legislation creating a safe harbour for researchers who act responsibly. The U.S. Department of Justice has publicly committed to not prosecute good-faith research under the Computer Fraud and Abuse Act (CFAA), and several U.S. states have codified security research defences.

Australia should amend the Criminal Code to establish a clear good-faith security research defence, with specific criteria such as no intent to harm, no data exfiltration, and prompt reporting. Reforms could also extend whistleblower protections to include cybersecurity-related disclosures in the public interest. The government can further promote the use of structured agreements (such as bug bounty terms or safe harbour clauses) that formalise authorisation for ethical testing.

A national VDP framework would not only provide legal certainty but also promote public-private collaboration and cyber resilience. Ethical hackers are among the most effective force multipliers in cybersecurity. HackerOne's global experience shows that when researchers are given a clear, safe path to disclosure, the volume and quality of reports rise and organisations are able to fix vulnerabilities long before they can be exploited.

Australia's 2023–2030 Cyber Security Strategy rightly aims to embed secure-by-design principles, boost critical infrastructure resilience, and partner with the private sector to uplift national cyber posture. A National Vulnerability Disclosure Framework anchored in clear law, strong policy, and operational support is a foundational step in delivering that vision.

* * *

HackerOne thanks the Department of Home Affairs for the opportunity to comment on the Horizon 2 Policy Discussion Paper and appreciates your consideration of our

recommendations. We strongly encourage the government to take the opportunity to align with vulnerability disclosure best practices emerging from international partners as part of developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.

Respectfully Submitted,

[redacted]

HackerOne