Dear Secretary Pezullo and the team at the Department of Home Affairs,

Thank you for the opportunity to provide feedback on the paper Strengthening Australia's Cyber Security Regulations and Incentives.

To begin, the Bugcrowd team, the security researcher community, and I all applaud this endeavor. In 2012, I founded Bugcrowd, an Australian-founded company that was the first to operationalize and mediate the relationship between the hacker community and organizations seeking their input through our expert team and proprietary platform.

Since then, we've raised $80 million in venture capital, opened offices in Sydney, San Francisco, London, and other cities around the world, hired 250,000+ helpful hackers from around the world, and collaborated with organizations ranging from the US Department of Defense, the Department of Homeland Security, Mastercard, Microsoft, Facebook, National Australia Bank, Atlassian, and many more.

The mission of "Making Australia's Digital Economy More Resistant to Cyber Security Threats" is very similar to Bugcrowd's core mission of "Making the Digital World Safer."

The DOHA action pillars of clear expectations, increased transparency and disclosure, and customer rights protection are fundamental to why we started Bugcrowd in the first place, to create a platform to facilitate these actions by enabling the collective creativity of the security research and benevolent vulnerability finder community as a latent but enormously powerful ally.

The information systems that power the Australian government and businesses are the result of human ingenuity and hard work. Humans, while unparalleled in terms of creativity and ability to pursue potential, are also fallible, which creates vulnerabilities and risks. This is simply a side effect of being human. This truism begs the question of how to identify, fix, and reduce the likelihood of these risks in the future, before the adversary discovers and exploits them.

Those with the skills and altruistic interest in identifying cyber risk and improving the safety and security of the Internet have been patiently waiting for the better part of 30 years, and our efforts to assist have received varying responses. Many of them were fearful, hostile, and negative until about 6 or 7 years ago. The evolution of the information attack surface and the capabilities of our adversaries has resulted in a significant shift: the Internet realized that not all "hackers" are burglars; in fact, many of them are locksmiths.

Simply put, there is a crowd of people building software and systems, and a crowd of people working to find new ways to attack our software and systems, and the DOHA paper (particularly the components dealing with responsible disclosure) proposes what we believe to be a logical response: enlisting the crowd of good-faith hackers and concerned Netizens to assist the government in defending its information.

The recommendations below are based on our experience with a wide range of organizations, which we believe reflects the range of agencies that would be covered by this paper. In general, we find the recommendations to be thoughtful and well-thought-out, and we are excited by the groundswell of support from the research and information security communities.

Because the average citizen is now aware of the risk of a cyberattack, it has become a sociopolitical issue, as it has a direct impact on the constituent's trust in their government.
The transparency and conceptual simplicity of "Neighborhood watch for the Internet" are a natural fit to the overarching issue of constituent confidence, but our experience strongly suggests that the journey to maturity in a vulnerability disclosure program is not one-size-fits-all. A methodical approach is required to ensure a smooth implementation and successful outcomes.

As a result, our recommendations focus on maximizing whole-of-program success while taking individual agency and organizational needs into account in the implementation of the paper's recommendations.

Recommendations:

Consider policy-driven mandates for Federal agencies to implement vulnerability disclosure programs (VDPs).

- VDPs are now widely recognized in security and technology circles, though the level of understanding and acceptance varies depending on organizational and individual experience.
- Despite the lack of a public and proactive policy and report intake channel, many agencies are already receiving reports of vulnerabilities, and the frequency with which this is occurring is increasing. In this scenario, vulnerability reports are frequently ignored or routed to aggregators such as ACSC or AusCERT, increasing the likelihood that identified issues will go unresolved.
- Our experience in APAC and the US suggests that a top-down mandate to "get the ball rolling" is the most effective and orderly way to drive adoption.
- The Hack The Pentagon programs, as well as the more recent DHS/CISA Federal Civilian programs (https://bugcrowd.com/programs/organizations/cisa) triggered by Binding Operational Directive 20-01, are examples of this.
- In both cases, these programs not only increased adoption in the target agencies, but also signaled the validity, safety, and importance of proactive security to other State and Local government agencies, as well as the corporate sector.
- This "trickle-down excellence" effect, in our opinion, is available and easily accessible to the Australian government.

Emphasize the cost-effectiveness of VDP compared to other security controls.

- According to the AustCyber sector competitiveness plan (https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3), there is a severe shortage of job-ready cyber security workers in Australia, which is consistent with similar studies from around the world.
- This deficit raises the cost of access to skills, resulting in a digital landscape skewed in favor of the adversary.

- Inviting the input of the broader security research community via a platform like Bugcrowd is a safe and flexible approach to leveling the resourcing and economic advantage possessed by attackers, and program management is cost-effective (https://tracker.bugcrowd.com/products/pricing/vulnerability_disclosure).

Provide clear guidelines for best practices in voluntary adoption.

- The answer to the question "how" is frequently the limiting factor in VDP adoption.
- In addition to the above-mentioned mandate, the Australian government could follow the lead of CISA/DHS and 18F in the United States by making as much guidance on successful VDP implementation as possible public. This has the dual effect of assisting Federal agencies in their adoption while also providing a clear set of starting principles for use by businesses and non-federal agencies.
- CISA's "GUIDE TO VULNERABILITY REPORTING FOR AMERICA'S ELECTION ADMINISTRATORS" (https://www.cisa.gov/sites/default/files/publications/guide-vulnerability-reporting-americas-election-admins 508.pdf) was used outside of the election space due to its clarity, authority, and cross-industry utility.

Ensure that safe harbor is as simple to understand and apply as possible.

- Existing anti-hacking laws, both federal and state, have traditionally relied on a presumption of malice if unauthorized access is attempted or obtained.
- While actual prosecution for good-faith security research has decreased, deliberate efforts to align the intent of programs like the DOHA paper within and across participant organizations, as well as deliberate signaling of this intent to the security community, remain critical.
- Efforts to standardize, simplify, and promote the significance of authorization and Safe Harbor language can be found at https://policymaker.disclose.io if additional language to address DMCA, State laws, Terms of Service, or other considerations is required.

Consider combining the VDP recommendation with smart device labeling and consumer safeguards.

- Unlike many defensive cybersecurity controls, VDP's role as "Neighborhood Watch for the Internet" is both simple to understand for the layperson and indicative of an organization's cybersecurity maturity in a way that can easily be leveraged into increased consumer trust.
- For example, Facebook, Google, Apple, and Microsoft have all proactively positioned their openness to receiving security feedback to the market since 2010, and are widely regarded as cutting-edge and trustworthy when it comes to data security.
- For example, Bugcrowd collaborated with the Capitol House Rules Committee, DHS/CISA, the National Association of State Secretaries, and a slew of other organizations to incorporate VDP into the 2020 US General Elections ahead of the threat of system confidence attacks. This strategy proved effective in combating disinformation in late 2020 and early 2021 (https://venturebeat.com/2020/10/23/how-ethical-hackers-protect-2020-us-elections/).

- This opens up the possibility of incentives: The presence or absence of a VDP is a natural and logical data point to feed into the paper's smart device labeling recommendation, and it could be incorporated into consumer protections as a modifier to punitive actions in the event of a breach.

Distinguish "vulnerability disclosure" from "bug bounty" and "private crowdsourced security" clearly.

- It is critical to distinguish between vulnerability disclosure programs and bug bounties, and this must be done early and frequently.
- This disambiguation is critical because it prevents agencies and organizations that conflate the concept with bug bounty programs from dismissing VDP as a non-starter, as well as hasty adoption by those who conflate the concept with private crowdsourced security.
- This also clarifies that one of the primary goals of a VDP is communication, transparency, and trust.

Consumer understanding of cybersecurity threats is a relatively new phenomenon, and it has resulted in a greater desire for transparency in the measures being taken to protect consumer data and the digital workflows that impact almost every conceivable aspect of life at this point.

We'd like to express our appreciation and commendation for DOHA's efforts on this paper, and it's recommendations. This effort legitimizes the security researcher community, promotes transparency and pragmatism in vulnerability management within government agencies, and will result in a more resilient digital economy for Australia.

We are prepared to provide additional input and assistance as needed to support this initiative.

Kindest regards,

Casey Ellis
Founder, Chairman, and CTO - Bugcrowd

[redacted]
https://bugcrowd.com
[redacted]