hackerone

September 15, 2020

**SUBMITTED VIA SUBMISSION FORM**

The Honorable Peter Dutton MP
Minister for Department of Home Affairs
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

**Re: Protecting Critical Infrastructure and Systems of National Significance - Consultation Paper**

Dear Minister Dutton:

HackerOne Inc. ("HackerOne")[1] submits this letter in response to the request for comment on the Australian Government's Department of Home Affairs draft consultation paper on Protecting Critical Infrastructure and Systems of National Significance ("Consultation Paper").[2] Specifically, we would like to provide a response to the following questions from the Consultation Paper's Call for views:

> 22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?
>
> 25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

HackerOne is the market leading hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. We are proud to work with over 10,000 Australia-based security researchers who have collectively made the internet safer through the discovery of over 7,300 vulnerabilities. The implementation of vulnerability disclosure policies ("VDPs") throughout Australia's critical infrastructure will assist Australia's most important entities in proactively identifying and remediating cyber vulnerabilities, including those at the perimeter of critical networks.

A full discussion of VDPs and other governments' successes with them appears below.

[1] HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.

[2] Protecting Critical Infrastructure and Systems of National Importance Consultation Paper, *available at* https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf.

### A. The Importance of VDPs

A vulnerability disclosure policy, or VDP, is an organization's formalized method for receiving vulnerability submissions from the outside world. A VDP is intended to give finders—anyone who stumbles across something amiss (aka "researchers", "hackers", "security researchers")—clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible. This practice is defined and outlined in a number of different government and non-government publications, including:

- European Telecommunications Standards Institute's ("ETSI") European Standard ("EN") 303 645 v2.1.1;[3]
- International Organization for Standardization ("ISO") Standard 29147;[4]
- U.S. Department of Justice's ("DOJ") *Framework for a Vulnerability Disclosure Program for Online Systems*;[5] and,
- U.S. National Telecommunications and Information Administration's ("NTIA") *"Early Stage" Coordinated Vulnerability Disclosure Template*.[6]

Each of these documents emphasizes the importance of instituting formal VDPs and provides a framework to do so. For example, the NTIA *Template* notes, "[w]ith softened fear of legal concerns, higher numbers of researchers are likely to engage in vulnerability research and disclosure," and stresses the need for organizations to "understand how the security research community may want to engage to equip themselves with a flexible set of tools to successfully collaborate and improve security."[7]

Generally, there are five key components of a VDP:

- **Promise**: Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities;
- **Scope**: Indicate what properties, products, and vulnerability types are covered;

[3] ETSI EN 303 645 at Provision 5.2 (2020-06), *available at* https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

[4] ISO/IEC 29147:2018 ("Information technology -- Security techniques -- Vulnerability disclosure"). The standard details the methods a vendor should use to address issues related to vulnerability disclosure.

[5] *A Framework for a Vulnerability Disclosure Program for Online Systems* (v1.0), DOJ (July 2017), *available at* https://www.justice.gov/criminal-ccips/page/file/983996/download.

[6] *"Early Stage" Coordinated Vulnerability Disclosure Template* (v1.1), NTIA SAFETY WORKING GROUP (Dec. 15, 2016), *available at* https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf.

[7] *Id.* at 3.

- **Safe Harbor**: Assures that reporters of good faith will not be unduly penalized;
- **Process**: The process finders use to report vulnerabilities; and,
- **Preferences**: A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

A well-established VDP also can be coupled with a bug bounty program (BBP), which is an organization's bounty-driven rewards program inviting a select group of hackers (private BBP) or any hacker (public BBP) to find exploits and vulnerabilities in its systems. A BBP is a proactive challenge to identify bugs by actively encouraging the security community to target select assets. When VDPs and BBPs are implemented in a progressive fashion, they are commonly seen as the most resourceful and cost-effective way to identify and ultimately remediate cyber vulnerabilities. However, they are fundamentally two different security exercises, and, for the purposes of securing critical infrastructure and systems of national importance, a VDP is a well-accepted start to engagement with security researchers.

## B. The Precedent of Mandated VDPs

The practice of vulnerability disclosure is becoming an increasingly significant component of any organization's risk-based security program. The U.S. government recently set a precedent by requiring all of its Federal agencies to have a VDP in place by March 1, 2021.[8] The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's ("CISA") binding operational directive ("BOD"), in particular, raises the baseline of security for the U.S. government as a whole by detailing the overarching approach agencies must take to address cybersecurity vulnerabilities. In addition to requiring each agency to add a security contact for each .gov domain registered, CISA's BOD requires an agency's VDP to have within its scope all internet-accessible systems or services by September 2022.

The United Kingdom is set to follow suit with respect to consumer smart products. It's Department for Digital, Culture, Media & Sport is currently working on regulations that would require, among other things, VDPs for any Internet of Thing manufacturer selling smart products to UK consumers.[9] Finally, the National Institute of Standards and Technology, the U.S. government's standards agency, has published a Framework for Improving Critical Infrastructure

[8] *See* "Improving Vulnerability Identification, Management, and Remediation" (M-20-32), U.S. OFFICE OF MGMT. AND BUDGET (Sep. 2, 2020), *available at* https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf; Binding Operational Directive 20-01, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *available at* https://cyber.dhs.gov/bod/20-01/.

[9] *Proposals for Regulating Consumer Smart Product Cyber Security - Call for Views*, DEP'T FOR DIGITAL, CULTURE, MEDIA & SPORT (July 16, 2020), *available at* https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views.

[10] *Framework for Improving Critical Infrastructure Cybersecurity* (v1.1), NIST (April 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Cybersecurity that includes a reference to public vulnerability disclosure as a necessary component of any organization's risk assessment program.[10]

### C. VDPs in Australian's Critical Infrastructure

VDPs would assist in proactively identifying and remediating cyber vulnerabilities, including those at the perimeter of critical networks. First, a VDP would assist in proactively identifying and remediating cyber vulnerabilities by welcoming collaboration from security contributors and researchers who are able to work beyond an organization's limitations to proactively identify vulnerabilities much faster than traditional, internal vulnerability detection means (e.g., penetration testing). With clear channels for outside security researchers to report vulnerabilities, teams within a critical infrastructure's organization will then be able to acknowledge the vulnerability and remediate it much faster than if there was no established reporting channel. All of this helps to amplify the notification and action organizations can take to address vulnerabilities on an expedited timeline.

Second, the nature of vulnerability testing conducted by an external security researcher inherently relies on the use of multiple detection practices to discover vulnerabilities. This is different from an internal prescribed vulnerability program where the tools and methodologies used would be singular in technology and personnel conducting the testing. This variation in different testing techniques, tools, and personnel involved allows for quality vulnerability detection that, again, often outshines vulnerability detection results from more traditional and single trajectory means, especially for vulnerabilities at the perimeter of critical networks.

With the many benefits inherent in establishing a baseline requirement for organizations to build trust through transparency and ensure their approach to cybersecurity is as collaborative as possible, the Australian government should join the United States and the United Kingdom in requiring VDPs in its critical infrastructures.

* * *

There is enormous societal value in hacker-powered security—i.e., any cybersecurity-enhancing services and automations that are partially or wholly produced by independently operating security experts outside of the company or organization. At scale, hacker-powered security has the opportunity to detect every hole, every weakness, and every security vulnerability in a system or product built by humans. HackerOne therefore urges the Australian Government's Department of Home Affairs to add a VDP component to any enhanced regulatory framework that will be introduced in connection with the Consultation Paper.

HackerOne thanks you for considering its comments. Should you have any questions, please contact us at [redacted] and [redacted].

Sincerely,

[redacted]

Kayla Underkoffler
Technology Alliances Manager
HackerOne

[redacted]

Alex Rice
Chief Technology Officer
HackerOne