hackerone

September 3, 2020

SUBMITTED VIA E-MAIL

The Honorable Matt Warman MP
Minister for Digital Infrastructure
100 Parliament Street
London
SW1A 2BQ

Re: Proposals for Regulating Consumer Smart Product Cyber Security – Call for Views

Dear Minister Warman:

HackerOne Inc. ("HackerOne") respectfully submits this letter in response to the call for views on the Department for Digital, Culture, Media & Sport's ("Department's") proposals for regulating consumer smart product cyber security ("Proposal").[1] We strongly commend the Department's robust discussion of vulnerability disclosure policies ("VDPs") in Requirement 2 of the Proposal.[2]

HackerOne is the market leading hacker-powered security platform, helping organisations find and fix critical vulnerabilities before they can be exploited. HackerOne is headquartered in San Francisco (United States) with offices in London, New York, the Netherlands, and Singapore. HackerOne is proud to work with the National Cyber Security Centre ("NCSC") on its VDP,[3] as well as with over 15,600 UK-based security researchers who have collectively made the internet safer through the discovery of over 73,700 vulnerabilities. The hacking community in the UK currently ranks 4th in the world, behind the USA, India and Russia, and marginally above the fast-growing communities in China and Germany.

As the Department previously noted, "[o]ver 90% of 331 manufacturers, supplying the UK market, reviewed in 2018 did not possess a comprehensive vulnerability disclosure programme up to the level we would expect," and that "[w]hilst the UK Government has previously encouraged industry to adopt a voluntary approach, it is now clear that decisive action

---

[1] *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 [hereinafter "Proposal"].

[2] *Id.* at § 3.3, Requirement 2.

[3] *NCSC UK*, HACKERONE, *available at* https://hackerone.com/ncsc_uk.

is needed to ensure that strong cyber security is built into these products by design."[4] Mandating VDPs via legislation and citing to other official UK government, United States government, and non-governmental guidance will ensure that critical elements of VDPs are implemented in a consistent manner and in accordance with how these tasks are understood in other contexts.

A. The Importance of VDPs

A vulnerability disclosure policy, or VDP, is an organisation's formalised 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;[5]
- International Organization for Standardization ("ISO") Standard 29147;[6]
- U.S. Department of Justice's ("DOJ") *Framework for a Vulnerability Disclosure Program for Online Systems*;[7] and,
- U.S. National Telecommunications and Information Administration's ("NTIA") *"Early Stage" Coordinated Vulnerability Disclosure Template*.[8]

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 organisations to "understand how the security research

---

[4] *Government Response to the Regulatory Proposals for Consumer Internet of Things (IoT) Security Consultation*, DEP'T FOR DIGITAL, CULTURE, MEDIA & SPORT (July 16, 2020), *available at* https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation.

[5] 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. *See also* Proposal, *supra* note 1, at Requirement 2.

[6] 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.

[7] *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.

[8] *"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.

community may want to engage to equip themselves with a flexible set of tools to successfully collaborate and improve security."[9]

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;
- **Safe Harbor**: Assures that reporters of good faith will not be unduly penalised;
- **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.

VDPs offer alternatives to prescriptive regulation, are adaptable measures that can be modified over time, and generate outcome-based efficacy. They also are already being integrated as best practices into many entities' cybersecurity frameworks. The Proposal rightfully recognizes this industry practice and promotes the adoption of VDPs in Requirement 2.

B. The U.S. Government's Success with VDPs

The U.S. government's previous successes with VDPs– including their use within the U.S. Department of Defense ("DoD")[10] – and the requirement that all U.S. Federal agencies publish VDPs pursuant to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's ("CISA") binding operational directive[11] provide a proven track-record that mandating cybersecurity tools via legislation works.

The DoD's VDP has become both the benchmark and model for the entire U.S. Federal government with over 14,000 valid vulnerabilities reported in government systems; almost 3,000 in its third year alone. As DoD Cyber Crime Center's ("DC3") Executive Director Jeffrey D. Specht explains in DC3's latest annual VDP report:

> In 2019, [2,836 valid vulnerabilities were discovered by DoD VDP]. These vulnerabilities were previously unknown to the DoD and not found by automated network scanning software, red teams, manual configuration checks, or cyber inspections. Without DoD VDP there is a good chance those vulnerabilities

[9] *Id.* at 3.

[10] The DoD's VDP with HackerOne can be viewed at https://hackerone.com/deptofdefense.

[11] *See* CISA Binding Operational Directive 20-01, *available at* https://cyber.dhs.gov/bod/20-01/.

would persist to this date, or worse, be active conduits for exploitation by our adversaries.[12]

Furthermore, CISA recently finalized a binding operational directive that requires all U.S. Federal agencies to develop and publish their own VDPs.[13] HackerOne believes that the UK government should similarly require these cybersecurity tools be incorporated into legislation regulating consumer smart products sold in the UK.

C. VDPs Should be an Explicit Part of UK Legislation

As exemplified by the actions already taken by the U.S. DoD and CISA, the UK government is right to be thinking holistically to reduce, mitigate, and address vulnerabilities. To this end, HackerOne urges you to maintain in any proposed legislation references to VDPs as stated in Requirement 2.

HackerOne further suggests that the legislation require in-scope manufacturers to commit "to not recommend or pursue legal action against anyone for security research activities that the [manufacturer] concludes represents a good faith effort to follow the policy, and *deem that activity authorized*."[14] The legislation could go further and require the manufacturer "not to pursue civil action for accidental, good faith violations of its policy or initiate a complaint to law enforcement for unintentional violations. . . . If legal action is initiated by a third party against a party who complied with the vulnerability disclosure policy, the [manufacturer] will take steps to make it known, either to the public or to the court, that the individual's actions were conducted in compliance with the policy."[15]

For example, the vulnerability disclosure policy of Her Majesty's Royal Air Force[16] states: "*The RAF affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a RAF service or system, where the researcher has acted in good faith and in accordance with this disclosure policy.*"

Finally, to ensure that critical elements of VDPs are implemented in a consistent manner and in accordance with how these tasks are understood in other contexts, HackerOne recommends that the legislation (or accompanying legislative history / guidance) continue to cite

---

[12] *DC3 VDP Annual Report 2019 (Volume 1)*, DoD, *available at* https://www.dc3.mil/Portals/100/Documents/DC3/Directorates/VDP/Annual%20Reports/2019_vdp_annualmetricvol1.pdf.

[13] *See CISA Issues Final Vulnerability Disclosure Policy Directive for Federal Agencies*, CISA (Sep. 2, 2020), https://www.cisa.gov/news/2020/09/02/cisa-issues-final-vulnerability-disclosure-policy-directive-federal-agencies.

CISA Binding Operational Directive 20-01, *available at* https://cyber.dhs.gov/bod/20-01/.

[14] *Id.* (emphasis in original).

[15] *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.

[16] https://www.raf.mod.uk/privacy/vulnerability-reporting/

official guidance on VDPs. HackerOne applauds the Proposal's reference to ETSI EN 303 645 and ISO 29147.[17] To further ensure successful implementation, reference also could be made to National Institute of Standards and Technology ("NIST") Special Publication 800-53, Revision 5,[18] and CISA's excellent VDP Implementation Guide and the "prior art" contained in it.[19]

* * *

HackerOne thanks you for considering its comments. Should you have any questions, please contact me at alex@hackerone.com.

Sincerely,

Alex Rice

Alex Rice
Chief Technology Officer
HackerOne

[17] Reference to ISO 30111 also should be considered. *See* ISO/IEC 30111:2013 ("Information technology -- Security techniques -- Vulnerability handling processes").

[18] Draft NIST Special Publication 800-53, Revision 5 (Final Public Draft), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf.

[19] *See CISA Binding Operational Directive 20-01 Implementation Guide*, *available at* https://cyber.dhs.gov/bod/20-01/#implementation-guide.