hackerone

June 08, 2021

SUBMITTED VIA E-MAIL

The CMA Review
Home Office
2 Marsham Street
London
SW1P 4DF

Re: Computer Misuse Act 1990 – Call for Information

Dear Rt Hon Priti Patel, MP:

HackerOne Inc. ("HackerOne") respectfully submits this letter in response to the call for information on the Home Office's Computer Misuse Act 1990 ("CMA").[1] We commend the Home Office's commitment to reviewing the 30-year-old legislation with a keen eye toward meeting the future needs of UK law enforcement, citizens, businesses, and security researchers.

HackerOne is the world's most trusted hacker-powered security platform, connecting organizations to the largest community of hackers on the planet to find and safely report security weaknesses across attack surfaces. HackerOne is headquartered in San Francisco (United States) with offices in London, New York, and the Netherlands. In the UK, HackerOne works with entities in the public and private sectors such as Costa Coffee, Starling Bank, and the National Centre for Cyber Security ("NCSC"). The ethical hacking community in the UK currently ranks 4th in the world, behind the USA, India, and Russia.

As a champion for the security community at large, HackerOne is of the opinion that this CMA update must address the restrictions this legislation currently places on legitimate third party security researchers and the act of reporting vulnerabilities in good faith. The revision of the CMA should make it clear and unquestionable that the operation of a VDP, and the act of reporting a vulnerability through that VDP, is a sanctioned and encouraged practice that does not conflict with the purpose and intent of the CMA. In essence, VDPs should become the de facto channel for security researchers to communicate vulnerabilities and security gaps to organizations. HackerOne encourages the Home Office to incorporate and legitimize VDPs through the CMA legislation as the single best channel for responsible reporting of vulnerabilities and security issues to organizations. Our thoughts and arguments are presented below.

A. Vulnerability Disclosure

[1] *Computer Misuse Act 1990 - Call for Information*, HOME OFFICE (May 11, 2021), *available at* https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information.

A VDP (sometimes called "responsible disclosure" or "Coordinated Vulnerability Disclosure") 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. When these policies are in place, there is implicit protection for third party researchers who report vulnerabilities discovered in good faith, and likewise, there are protections in place for the organizations who host the policy.

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 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.

This practice is well defined and outlined in a number of government and non-government publications, and there are strong examples of successful VDPs that have benefited both the hosting organizations and security researchers. Some UK Government specific examples include the VDPs for The Ministry of Defense ("MOD")[2] and the UK's NCSC[3]. The safe harbor inclusion for the MOD VDP is an excellent example of language that clarifies protections in place for security researchers:

> "The MOD affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a MOD service or system, where the researcher has acted in good faith and in accordance with this disclosure policy."

While there are many established examples of the benefits of VDPs, the lack of clarity in the current CMA legislation can unintentionally elicit fear that even sanctioned programs may be operating in violation of the CMA, despite the fact they're perfectly legitimate. HackerOne has even developed standard safe harbor components for customers who specifically choose to include the CMA as a reference law. An example of that language was in the Royal Air Force VDP language prior to the program being included within the MOD VDP. The language reference is as follows:

---

[2] *Vulnerability Disclosure Policy,* MINISTRY OF DEFENSE (December 2, 2020), *available at* https://www.gov.uk/guidance/report-a-vulnerability-on-an-mod-system.

[3] *Vulnerability Disclosure Policy,* UK NATIONAL CYBER SECURITY CENTRE (November 15, 2018), *available at* https://hackerone.com/ncsc_uk.

"This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the RAF to be in breach of any of its legal obligations, including but not limited to:

- The Computer Misuse Act (1990)
- The General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018
- The Copyright, Designs and Patents Act (1988)
- The Official Secrets Act (1989)

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."

These safe harbor components are built-in to encourage researchers to disclose vulnerabilities without hesitation. As stated above, this revision of the CMA should make it clear and unquestionable that the operation of a VDP, and the act of reporting a vulnerability through that VDP, is a sanctioned and encouraged practice that does not conflict with the purpose and intent of the CMA. In essence, VDPs should become the de facto channel for security researchers to communicate vulnerabilities and security gaps to organizations.

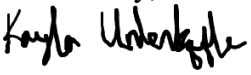
B. VDP – Protection for All

Again, HackerOne encourages the Home Office to incorporate and legitimize VDPs through the CMA legislation as the single best channel for responsible reporting of vulnerabilities and security issues to organizations. Additionally, those VDPs should be clearly approved as a practice in line with public interest. This commitment to protecting legitimate security research through the practice of vulnerability disclosure should be clearly outlined within the CMA and should encourage organizations to establish VDPs to help foster the culture of responsible vulnerability disclosure.

* * *

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

Sincerely,



Kayla Underkoffler
Technology Alliances Manager
HackerOne