hackerone

December 14, 2022

SUBMITTED VIA ELECTRONIC FILING – www.regulations.gov

Mr. Richard Ifft
Senior Insurance Regulatory Policy Analyst
Federal Insurance Office
Room 1410 MT
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Re: HackerOne Comments on "Potential Federal Insurance Response to Catastrophic Incidents" --- Docket ID TREAS-DO-2022-0019

Dear Mr. Ifft:

HackerOne Inc. ("HackerOne") submits this letter in response to the Federal Insurance Office's ("FIO's") request for comment on the notice on Potential Federal Insurance Response to Catastrophic Incidents ("Notice").[1] We are pleased to see FIO's commitment to exploring measures to strengthen the cyber insurance market by addressing existing vulnerabilities in our current system and identifying solutions for mitigating catastrophic risk to critical infrastructure.

By way of background, HackerOne closes the security gap between what organizations own and what they can protect. HackerOne's Attack Resistance Management blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to find and close gaps in the ever-evolving digital attack surface. This approach enables organizations to transform their business while staying ahead of threats. Customers include The U.S. Department of Defense, Dropbox, General Motors, GitHub, Goldman Sachs, Google, Hyatt, Lufthansa, Microsoft, MINDEF Singapore, Nintendo, PayPal, Slack, Starbucks, Twitter, and Yahoo. In 2021, HackerOne was named as a "brand that matters" by Fast Company.

HackerOne has consistently advocated for widespread adoption of hacker-powered cybersecurity measures that have proven effective at mitigating cyber risk in both the commercial and government contexts. As a global leader in implementing and managing tailored programs for protecting governments and organizations from the most sophisticated adversaries, our response will focus on **Topic 3 – Cybersecurity Measures**. Regardless of the particular federal cyber insurance program structure that may be recommended by FIO, HackerOne suggests three powerful cybersecurity and cyber hygiene measures that should be required of policyholders: Vulnerability Disclosure Programs ("VDPs"), Bug Bounty Programs ("BBPs"), and External Code Review. We address each cybersecurity tool in turn below.

Vulnerability Disclosure and Bug Bounty Programs

[1] U.S. Dep't Treas., Request for Comment, *Potential Federal Insurance Response to Catastrophic Cyber Incidents*, 87 Fed. Reg. 59161 (Sept. 29, 2022), *available at* https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents#addresses.

Vulnerability Disclosure Programs ("VDPs") are a foundational tool for entities to improve the security of their connected systems. A VDP is an organization's formalized method for receiving vulnerability submissions from the outside world. It is a reactive form of receiving bugs: organizations (usually through their third-party partners) accept the work of the security community and then work to address the vulnerabilities uncovered. In other words, it is the digital equivalent of "if you see something, say something." It is intended to give anyone—ethical hackers (aka "researchers" or "finders"), or anyone who stumbles across something amiss—clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible.

The federal government is no stranger to VDPs in own their security programs. In 2020, the Office of Management and Budget ("OMB") and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") both finalized policies that require all federal agencies to develop and publish their own VDPs.[2] CISA's binding operational directive in particular positioned VDPs as a crucial part of any cybersecurity strategy.[3] In May 2021, President Joe Biden issued an executive order on cybersecurity that instructed the federal government to, among other things, develop VDPs that include a reporting and disclosure process.[4]

Notably, we are increasingly witnessing various governments, agencies, and independent organizations recommending or mandating that businesses implement a VDP.[5] Unfortunately, many businesses have yet to implement these critical tools. According to our research, hackers often find bugs on organizations' websites, but 25% of the time they have no channel for alerting the organization that the bug exists. Even more worrisome, 82% of the Forbes Global 2000 do not have a known policy for vulnerability disclosure.[6] It therefore makes logical sense that a VDP requirement be extended to the cyber insurance market and, at absolute minimum, be required of all policyholders to mitigate potential breaches in their systems. Broad implementation of VDPs, particularly by entities that are economically linked and/or are integral to critical infrastructure, will go a long way toward reducing the likelihood of severe cyber incidents and the potential financial implication of such events.

Bug bounty programs serve as a powerful evolution of VDPs because they are both economically viable and highly effective for enhancing an entity's cyber security. A BBP is a bounty-driven rewards program where an organization invites any hacker (public BBP) or a select group of hackers (private BBP) to find exploits and vulnerabilities in its systems. It is a proactive

---

[2] *See* "Improving Vulnerability Identification, Management, and Remediation" (M-20-32), OMB (Sep. 2, 2020), *available at* https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf; CISA Binding Operational Directive 20-01, *available at* https://cyber.dhs.gov/bod/20-01/.

[3] *Id.*

[4] *Executive Order on Improving the Nation's Cybersecurity*, The White House (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[5] *See* VDPs are at the Heart of the Australian Cyber Security Centre's Recommendations (Dec. 8, 2020), available at https://www.hackerone.com/vulnerability-management/vdps-are-heart-australian-cyber-security-centres-recommendations.

[6] *See* The 4th Hacker-Powered Security Report (Sep. 21, 2020), available at https://www.hackerone.com/resources/reporting/the-4th-hacker-powered-security-report.

challenge to look for bugs by actively encouraging the security community through monetary rewards to target select assets. BBPs are a continuous security test that rewards ethical hackers for finding vulnerabilities and payment is made only when an in-scope vulnerability is found.

BBPs have been embraced at the federal level, most notably at the Department of Defense ("DoD") through the "Hack the Pentagon" program that ran in 2016. This initiative was the first BPP in the history of the U.S. government and it exceeded all expectations. The pilot program was designed to identify and resolve security vulnerabilities within DoD's public-facing websites through crowdsourced security. More than 1,400 participants registered, 250 eligible hackers submitted a vulnerability report, and 138 submissions were found to be "legitimate, unique and eligible for a bounty" and resolved, according to former Defense Secretary Ash Carter.[7] The increased adoption of BBPs across the federal government and the financial services industry suggests that these extremely effective tools should be a central part of any organization's cybersecurity infrastructure and should be designated a best practice when assessing an entity's risk profile for cyber insurance coverage.

External Code Review

The FIO should also consider requirements relating to source code review, a powerful tool for detecting vulnerabilities before they are released. In our experience, it is common to uncover vulnerabilities in applications that are already in use by an entity either due to weakness in the initial code, or introduction of bugs during updates. By implementing a code review program, an organization can take advantage of a team of third-party experts to review existing applications or software updates and provide an additional layer of protection to their code.

While identifying vulnerabilities is only part of an organization's security, implementing programs that prioritize detection of security weaknesses is critical for mitigating potentially catastrophic cyber events. At scale, hacker-powered security measures such as VDPs and BBPs, as well as external code review programs, have the potential to detect weaknesses and vulnerabilities before they pose any risk. These methods have proven to be extremely effective and are increasingly serving as critical pieces of cybersecurity infrastructure relied on by our federal government and organizations at home and abroad. We strongly encourage FIO to embrace these measures as required tools for eligibility of an impacted entity to make a claim against any federal catastrophic insurance offering.

HackerOne thanks you for considering its comments. Please do not hesitate to contact us for further information or if we may otherwise be of assistance.

Sincerely,

Ilona Cohen

Ilona Cohen
Chief Legal and Policy Officer
HackerOne

[7] *See* Hack the Pentagon, HackerOne, available at https://www.hackerone.com/hack-the-pentagon.