hackerone

June 23, 2023

SUBMITTED VIA ELECTRONIC FILING – www.regulations.gov

Cybersecurity and Infrastructure Security Agency (CISA)
Department of Homeland Security (DHS)

Re: HackerOne Response to "Request for Comment on Secure Software Development Attestation Common Form" --- Docket ID CISA-2023-0001

Dear Sir or Madam:

HackerOne Inc. (HackerOne) submits this letter in response to the Cybersecurity and Infrastructure Security Agency's (CISA) request for comment on the Secure Software Development Attestation Common Form (Form).[1] We are pleased to see CISA's commitment to implementing measures in Executive Order 14028 designed to improve cybersecurity standards and promote transparency in cybersecurity. Our comments recommend that CISA:

1. Clarify vulnerability disclosure policies and bug bounties are among the mechanisms that software producers can use to fulfill the attestation requirement of participation in vulnerability disclosure program; and

2. Clarify that source code review is among the mechanisms that software producers can use to fulfill the attestation requirement of maintaining trusted source code supply chains.

By way of background, HackerOne pinpoints the most critical security flaws across an organization's attack surface with continual adversarial testing to outmatch cybercriminals. HackerOne's Attack Resistance Platform blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to reduce threat exposure and empower organizations to transform their businesses with confidence. Customers include Citrix, Coinbase, Costa Coffee, General Motors, GitHub, Goldman Sachs, Google, Hyatt, Microsoft, PayPal, Singapore's Ministry of Defense, Slack, the U.S. Department of Defense, and Yahoo.

HackerOne has consistently advocated for widespread adoption of hacker-powered cybersecurity measures that have proven effective at addressing unmitigated vulnerabilities in both the commercial and government contexts. We further suggest the inclusion of External Code Review. We address each in turn below.

1. Clarify that vulnerability disclosure policies and bug bounty programs can be used to fulfill the vulnerability disclosure requirement.

[1] U.S. Dep't of Homeland Security, Request for Comment, *Request for Comment on Secure Software Development Attestation Common Form*, 88 Fed. Reg. 25670 (Apr. 27, 2023), *available at* https://www.federalregister.gov/documents/2023/04/27/2023-08823/agency-information-collection-activities-request-for-comment-on-secure-software-development.

HackerOne strongly supports the inclusion of vulnerability disclosure and management as an attestation requirement.[2] We recommend that CISA explicitly note—either on the Form or in related guidance—that software producers can fulfill the vulnerability disclosure requirement in multiple ways, including but not limited to Vulnerability Disclosure Policies (VDPs) and Bug Bounty Programs (BBPs).

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 "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 their own security programs. In 2020, the Office of Management and Budget (OMB) and CISA both finalized policies that require federal agencies to develop and publish their own VDPs.[3] CISA's own binding operational directive, in particular, positioned VDPs as a crucial part of any cybersecurity strategy.[4] In May 2021, President Joe Biden's Executive Order 14028 on cybersecurity instructed the federal government to, among other things, develop VDPs that include a reporting and disclosure process.[5]

Notably, we are increasingly witnessing various governments, agencies, and independent organizations recommending or mandating that businesses implement a VDP.[6] 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.[7] Including a VDP requirement in the Form helps address this gap for those seeking to provide software to the federal government. Broad implementation of VDPs, particularly by entities that are economically linked and/or are integral

---

[2] *See "*Secure Software Development Attestation Form Instructions," Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (Apr. 2023), pg. 6, *available at* https://www.cisa.gov/sites/default/files/2023-04/secure-software-self-attestation_common-form_508.pdf.

[3] *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/.

[4] *Id.*

[5] *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/.

[6] *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.

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

to the operation of the federal government, will go a long way toward improving the baseline cybersecurity of federal systems.

Bug bounty programs serve as a powerful evolution of VDPs because they are both economically viable and highly effective for enhancing an entity's cybersecurity. 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 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 initiated in 2016. This initiative was the first BBP 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. Most recently, in just seven days, the Hack U.S. BBP saw 648 reports submitted by 267 hackers, resulting in $75,000 in bug bounties and $35,000 in best of category challenge bonuses.[8] 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 recognized as a best practice when assessing an entity's secure software development compliance.

2. Clarify that external code review can be used to help fulfill requirements to maintain trusted source code supply chains.

CISA should also consider clarifying that organizations can use several processes, including source code review, to fulfill the attestation requirement to maintain trusted source code supply chains.[9] Source code review is a powerful tool for detecting vulnerabilities in software before it is 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

[8] *See* "Announcing the Results of Hack U.S.," HackerOne, available at https://www.hackerone.com/bounty/announcing-results-hack-us.

[9] *See* "Secure Software Development Attestation Form Instructions," Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (Apr. 2023), pg. 5, *available at* https://www.cisa.gov/sites/default/files/2023-04/secure-software-self-attestation_common-form_508.pdf.

and are increasingly serving as critical pieces of cybersecurity infrastructure relied on by our federal government and organizations at home and abroad.

* * *

As a global leader in implementing and managing tailored programs for protecting governments and organizations from the most sophisticated adversaries, we commend CISA for highlighting the importance of vulnerability disclosure and management to the development and continuous maintenance of secure software. We urge CISA to clarify that the vulnerability disclosure requirement can be fulfilled by several mechanisms, such as VDPs and BBPs. We further suggest that CISA include reference to source code review, including external code review, in the Form. 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