hackerone

July 7, 2022

VIA ELECTRONIC SUBMISSION TO: REGULATIONS.GOV

Division of Dockets Management
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20879

Re: Docket No. FDA-2021-D-1158. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions; Draft Guidance

To Whom It May Concern:

HackerOne appreciates the opportunity to comment on the Food and Drug Administration's ("FDA's") "Draft Guidance on Cybersecurity in Medical Devices and Quality System Considerations and Content of Premarket Submissions" ("Draft Guidance").[1]

HackerOne is a global leader in cybersecurity Attack Resistance Management ("ARM"), which closes the security gap between what organizations own and what they can protect. ARM 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. Our customers include the U.S. Department of Defense, General Motors, Goldman Sachs, Google, Hyatt, Microsoft, PayPal, and Twitter. HackerOne's global offices include its headquarters in San Francisco, with offices in London and the Netherlands.

HackerOne commends the FDA for its promotion of cybersecurity as part of medical device safety and the Quality System Regulations. This commitment is evident in the FDA's support of the Medical Device Innovation Consortium ("MDIC") report on coordinated vulnerability disclosure policies, medical device cybersecurity, and patient safety.[2] Cybersecurity vulnerabilities can pose serious risks for medical devices and patient safety, and HackerOne is committed to building a synergetic security ecosystem. The Draft Guidance appropriately recommends that manufacturers establish development processes that account for and address cybersecurity risks. HackerOne agrees with the FDA that "processes should address the identification of security risks, the design requirements for how the risks will be controlled, and the evidence that the controls function is designed and are effective in their environment of use for ensuring adequate security."[3]

---

[1] *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions; Draft Guidance for Industry and Food and Drug Administration Staff; Availability* (87 FR 20873) (Apr. 8. 2022).
[2] MDIC, *Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure* (Sept. 2018), http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf.
[3] Draft Guidance at 5.

Vulnerability Disclosure Is Essential. HackerOne has long been recognized as an industry-leader and subject matter expert on vulnerability disclosure. We strongly believe that independent third-party validation and a continuous review of the assumptions made in the original design are critical components of security by design as technology and digital societies evolve. We therefore urge FDA to include vulnerability disclosure programs ("VDPs") and bug bounty programs as a critical part of any mature security strategy. Today's cybersecurity challenges demand these tools.

In the software development lifecycle ("SDLC"), for instance, hacker-powered security can help. The Draft Guidance considers the adoption of a Secure Product Development Framework ("SPDF") as a way for manufacturers to manage cybersecurity risks.[4] While the SPDF processes help reduce the amount and severity of vulnerabilities in a product, including VDPs/bug bounty programs empowers companies to build a more security-aware engineering team that can work to close gaps before they are released. Indeed, by pushing security and vulnerability intelligence "to the left" in a SDLC, such continuous security helps protect future releases against threats. It prevents new products and applications from going into production with vulnerabilities. It also maximizes bounty program value to the organization and reduces the risk of future breaches. In other words, the same vulnerability reports used to drive improvements in the software production process can also ensure future code is continuously more secure.

Once a product goes to market, VDPs/bug bounty programs provide continuous security throughout the device's lifecycle. HackerOne's record of success – and that of its competitors – across widely diverse industries is proof positive that these programs are essential components of any cybersecurity defense. Equally as important to the inclusion of VDPs and bug bounty programs in the Draft Guidance is the emphasis on the cycle of new code releases. When the finding and fixing of new vulnerabilities can be crowdsourced, organizations are better equipped to educate their developers on not only fixing the code, but producing better code in the future.

We therefore urge FDA to elaborate on the Draft Guidance's short discussion of "Vulnerability Management Plans."[5] FDA should clearly set forth a description of the necessary elements of quality VDPs. We believe robust VDPs should:

- Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities;
- Indicate what properties, products, and vulnerability types are covered;
- Assure that reporters of good faith will not be unduly penalized;
- Clearly identify the process that researchers use to report vulnerabilities; and,
- Provide a living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

FDA will significantly strengthen the security posture of medical devices by expressly including robust VDPs/bug bounty programs in the Draft Guidance itself.

[4] *Id*. at 3.
[5] *Id.* at 27.

Code Review Is a Necessary Best Practice. Code review is essential to assessing the quality and security of the development process, and beyond. Accordingly, we propose that the Draft Guidance expand its recommendation for code review as a best practice beyond code that only "handles the parsing of external data."[6] Rather, the review should encompass all code and explicitly permit and encourage the use of third-party code review to supplement the device manufacturer's own security team of reviewers.[7]

Device manufacturers should have an established requirement for all applications that are submitted to undergo a code review to ensure the quality of the product's components meets the standards set by the organization. A code review can come in several forms. However, having a dedicated mechanism for device manufacturers to ensure this practice is a standard check in the process for all medical devices would go far to validate the promise of quality and security.

Updated Communications Plans. We agree with the Draft Guidance's proposal that vulnerability communication plans be part of pre-market submissions.[8] HackerOne does recommend, however, that the FDA update its recognition and recommendation of International Organization of Standards' ("ISO's") most recent standards relating to vulnerability handling and disclosure (ISO/IEC 29147:2014 to the updated 2018 standard; ISO/IEC 30111:2013 to the updated 2019 standard) and include them by reference within the Draft Guidance.[9] FDA should maintain guidance that accurately reflects the prevailing state of industry standards.

Again, HackerOne appreciates the opportunity to provide these comments. Please do not hesitate to contact us if we may provide more information or otherwise be of assistance.

Sincerely,

Michael Woolslayer
Lead Policy Strategist/Counsel

[6] *Id*. at 32.
[7] *Id*. at 31.
[8] *Id at 27*.
[9] *Postmarket Management of Cybersecurity in Medical Devices*, available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-managementcybersecurity-medical-devices. (*See* footnote 10).