hackerone

November 6, 2023

SUBMITTED VIA ELECTRONIC FILING – cyberframework@nist.gov

Cybersecurity Framework
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Public Draft of the NIST Cybersecurity Framework 2.0 Core with Implementation Examples

To Whom It May Concern:

HackerOne Inc. (HackerOne) submits the following comments in response to the National Institute for Standards and Technology (NIST) Public Draft of the Cybersecurity Framework (CSF) 2.0 Core with Implementation Examples.[1] HackerOne appreciates the opportunity to provide input, and we commend NIST for its openness and commitment to working with industry stakeholders to address the updates to the CSF.

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 Coinbase, General Motors, GitHub, Goldman Sachs, Hyatt, PayPal, Singapore's Ministry of Defense, and the U.S. Department of Defense.

HackerOne has consistently advocated for widespread adoption of vulnerability disclosure and vulnerability detection programs that have proven effective at addressing unmitigated vulnerabilities in both the commercial and government contexts.

Vulnerability Disclosure Policies

We commend NIST for incorporating ID.RA-08, formerly RS.AN-5, in this framework. This control includes a requirement to establish "processes for receiving, analyzing, and responding to vulnerability disclosures."[2] Such processes often take the form of vulnerability disclosure policies (VDPs), which create processes to document and submit security vulnerabilities. Undetected and unmitigated vulnerabilities pose a significant threat to the protection of sensitive data and the proper functioning of systems. VDPs play a crucial role in

[1] NIST, *Public Draft: The NIST Cybersecurity Framework 2.0*, Aug. 8, 2023, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf.
[2] NIST, *Public Draft: The NIST Cybersecurity Framework 2.0*, ID.RA-08, Aug. 8, 2023, pg. 35, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

enabling the prompt identification and reporting of vulnerabilities to software and systems owners and operators, facilitating swift remediation before cybercriminals and other bad actors have a window to exploit those vulnerabilities. VDPs can increase security without placing an undue burden on organizations. As noted in SP 800-53r5, "vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports."[3] In comparison to many other practices, VDPs are not especially complex or burdensome.

We strongly support NIST's incorporation of VDPs in CSF 2.0 which ensures alignment with existing requirements, best practices and international standards, such as NIST's own Cybersecurity Framework (CSF) 1.1[4], the CSF 2.0 Core discussion draft[5], and SP 800-53r5.[6]

Incorporate Bug Bounty Programs under the Identify Function

The Identify Function serves as a way to understand the current cybersecurity risk to an organization. NIST's recommendation of VDPs under the Identify Function is a significant step in the right direction, but we urge NIST to further recognize other valuable methods such as Bug Bounty Programs (BBPs) explicitly in CSF 2.0. BBPs serve as a parallel avenue for vulnerability scanning and, importantly, the identification and triaging of vulnerabilities within an organization's systems.

The fundamental difference between VDPs and BBPs lies in their approach to incentivizing security researchers. While both programs aim to identify vulnerabilities, BBPs take it a step further by compensating ethical hackers and security researchers for reporting in-scope vulnerabilities. By recognizing BBPs as a viable and effective option, organizations are encouraged to leverage this powerful tool to bolster their cybersecurity posture.

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. By implementing bug bounty programs as part of a holistic security program, organizations can benefit from the experience of the global ethical hacker community and test the security of their most important systems. 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.

Incentivizing human professionals to identify vulnerabilities simulates real attack conditions and can provide an in-depth assessment of the organization's exposures and defenses. As a result, we encourage NIST to consider including explicit reference to a properly scoped BBP as a tool to help achieve the goals of the Identity Function and the broader CSF.

[3] NIST, SP 800-53 Rev. 5, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, RS.AN-5, Apr. 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[5] NIST, *Discussion Draft of the NIST Cybersecurity Framework 2.0 Core*, ID.RA-09, Apr. 24, 2023, https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf.
[6] NIST, SP 800-53 Rev. 5, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

Conclusion

HackerOne appreciates the opportunity to provide recommendations to this public draft. As the conversation around this topic continues to evolve, we are available to provide further input if requested to help ensure that the Cybersecurity Framework continues to be a vital resource for organizations seeking guidance on consistent, effective cyber risk management practices globally.

Sincerely,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne