hackerone

September 10, 2020

SUBMITTED VIA E-MAIL

Dr. Walter G. Copan
Director and Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Re: NIST Special Publication 800-53B – Request for Comment

Dear Dr. Copan:

HackerOne Inc. ("HackerOne")[1] submits this letter in response to the request for comment on the National Institute of Standards and Technology ("NIST") draft Special Publication 800-53B ("SP 800-53B" or "Publication").[2] We previously submitted comments on NIST SP 800-53, Revision 5, and are thrilled to see the inclusion of vulnerability disclosure policies ("VDPs") in RA-5(11):[3]

> (11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM
>
> Establish an [*Assignment: organization-defined public reporting channel*] for receiving reports of vulnerabilities in organizational systems and system components.

The Federal government is no stranger to VDPs in their security programs, and the importance of VDPs in these programs has only continued to grow. Including VDPs in NIST SP 800-53, Revision 5 is an important step forward, and emphasizes NIST's commitment to promoting risk-based security controls as best practices that are widely accepted by all those who interact with Federal systems.

Accordingly, RA-5(11) also should be included across all security control baselines (low-impact, moderate-impact, and high-impact) in the Publication. If the "ultimate objective

[1] HackerOne is the market leading hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.

[2] Draft NIST Special Publication 800-53B (Final Public Draft), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B-draft.pdf.

[3] Draft NIST Special Publication 800-53, Revision 5 (Final Public Draft) at 237 (lines 10303-10313), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf.

[of NIST SP 800-53B] is to make the systems we depend on more penetration-resistant,"[4] not including this control could result in undesired negative effects for both the Federal government and the security researcher community.

A. The Federal Government's Move to Mandate VDPs

On September 2, 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.[5] CISA's binding operational directive ("BOD"), in particular, raises the baseline of security for the U.S. government as a whole. However, the BOD does not extend to agencies' third-party service providers.[6] It makes logical sense, though, that a VDP requirement be incorporated into those who serve the U.S. government.

Where CISA stops, NIST should step in. NIST SP 800-53B is the perfect vehicle in which to require government service providers to have in place VDPs of their own. Without the same VDP standard required across the entire supply chain, Federal agencies will face an increased burden to ensure their assets are protected and covered under their own VDPs. This creates unnecessary risk and overhead.

B. Minimizing Risk for Security Researchers

Another important consideration for any VDP implementation is the built-in safety of the security researcher community. Currently, with the mismatch between Federal agencies being required to implement VDPs and their vendors not being held to the same standard, security researchers will be at a higher risk of mistakenly testing an area of a software's bill of materials that is not in a VDP's scope.

No technology is created without dependencies, and each line item in a software's bill of materials has the potential to belong to a different vendor. Without the clear direction and authorization in a VDP of which components are in-scope for testing and which are not, there will be an inherit and increased risk that researchers test and identify a vulnerability that may be out of scope. It is imperative that authorization for good faith testing be provided comprehensively at all levels of the Federal supply chain. Including RA-5(11) and its VDP requirements in NIST 800-53B will ensure this protection reaches down to the vendor level.

* * *

There is enormous societal value in hacker-powered security—i.e., any cybersecurity-enhancing services and automations that are partially or wholly produced by

[4] NIST SP 800-53B, *supra* note 2, at xi.

[5] *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/.

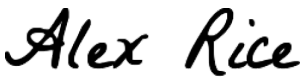
[6] *See id.* ("The directive does not grant your agency authority to force an organization you do business with to have a vulnerability disclosure policy.").

independently operating security experts outside of the company or organization. At scale, hacker-powered security has the opportunity to detect every hole, every weakness, and every security vulnerability in a system or product built by humans. HackerOne therefore urges NIST to add control RA-5(11) to all security control baselines (low-impact, moderate-impact, and high-impact) in the Publication.

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

Sincerely,

Kayla Underkoffler
Technology Alliances Manager
HackerOne



Alex Rice
Chief Technology Officer
HackerOne