hackerone

July 12, 2023

SUBMITTED VIA ELECTRONIC FILING – 800-171comments@list.nist.gov

National Institute of Standards and Technology (NIST)

Re: HackerOne Response to Request for Comment on NIST SP 800-171r3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

Dear Sir or Madam:

HackerOne Inc. (HackerOne) submits this letter in response to the National Institute of Standards and Technology's (NIST) updated draft guidelines for the NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.[1] We thank NIST for the opportunity to provide feedback on this critical issue.

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. HackerOne has consistently advocated for widespread adoption of vulnerability disclosure and vulnerability detection programs to identify and address unmitigated vulnerabilities effectively.

While HackerOne is largely supportive of NIST's updates to SP 800-171r3, we recommend the following changes:

1. **Incorporate vulnerability disclosure policies into SP 800-171 controls.**

2. **Allow for properly scoped bug bounties to fulfill scanning requirements set out in Control 3.11.2, *Vulnerability Monitoring and Scanning*.**

Incorporate Vulnerability Disclosure Policies

We strongly recommend that NIST update SP 800-171 control 3.11.2 to incorporate vulnerability disclosure policies (VDPs), as articulated in the RA-5(11) control to SP 800-53r5.[2] Undiscovered or unmitigated vulnerabilities are a direct threat to the confidentiality of sensitive information. VDPs play a crucial role in ensuring vulnerabilities are reported to software and system owners and operators so that vulnerabilities can be mitigated to protect the confidentiality of sensitive information. While the draft 3.11.2 control to SP 800-171r3 includes proactive vulnerability monitoring and scanning, the draft control excludes communication channels to receive vulnerability disclosures from unsolicited sources. Yet, as noted in SP 800-216,

[1] NIST, *SP 800-171 Rev. 3* (Draft), May 10, 2023, https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft.
[2] NIST, *SP 800-53 Rev. 5*, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

vulnerabilities are discovered by a variety of sources and, "regardless of who finds these vulnerabilities, it is critical that they are reported."[3]

Incorporating VDPs into SP 800-171 would not create 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."[4] In comparison to other practices required under SP 800-171, VDPs are not especially complex.

Incorporating VDPs into SP 800-171r3 would create more alignment with existing requirements and best practices for organizations processing sensitive information. NIST has previously recognized the importance of VDPsto discovery and remediation of vulnerabilities in documents such as the NIST Cybersecurity Framework (CSF) 1.1[5], the CSF 2.0 Core discussion draft[6], and SP 800-53r5.[7] VDPs are also incorporated into many other standards and requirements, including requirements for all federal agencies to develop and publish their own vulnerability disclosure policies,[8] and emerging secure software development requirements for government contractors.[9]

Despite its importance and increased use across the federal government, VDPs are not explicitly referenced in the current draft of SP 800-171. The lack of explicit reference in SP 800-171r3 diverges from cybersecurity best practices, as well as requirements for government agencies and some federal contractors. HackerOne urges that NIST update SP 800-171r3 control 3.11.2 to include an explicit reference to VDPs, in alignment with existing NIST guidance and widely adopted international standards.

Incorporate Bug Bounty Programs

As a global leader in implementing and managing tailored programs for protecting governments and organizations from the most sophisticated adversaries, we understand how important vulnerability monitoring and scanning is for the confidentiality of controlled unclassified information (CUI).

We urge NIST to update draft 800-171r3 control 3.11.2 to clarify that bug bounty programs (BBPs) are a practice for vulnerability scanning, as well as a source for identifying vulnerabilities for which to scan. This clarification would be consistent with guidance in the 800-53r5 control

[3] NIST, SP 800-216, *Recommendations for Federal Vulnerability Disclosure Guidelines*, May 2023, pg. 2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216.pdf.
[4] NIST, SP 800-53 Rev. 5, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[5] 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.
[6] 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.
[7] NIST, *SP 800-53 Rev. 5*, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[8] Office of Management and Budget, *M-20-32*, Sep. 2, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf.
[9] Department of Homeland Security, *Secure Software Development Attestation Form Instructions*, Draft, pg. 6, Apr. 27, 2023, https://www.cisa.gov/sites/default/files/2023-04/secure-software-self-attestation_common-form_508.pdf.

RA-5.[10] Control 3.11.2 specifies that it is the "organizations [choice to] determine the required vulnerability scanning for system components and ensure that potential sources of vulnerabilities are not overlooked."[11] While control 3.11.2 highlights the importance of different vulnerability analysis practices and vulnerability scanning tools, BBPs are not incorporated into the current draft of SP 800-171.[12] HackerOne suggests that NIST explicitly references BBPs as one of several viable options to fulfill the control's scanning requirements.

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.

Bug bounty programs also hold a competitive advantage over automated vulnerability scanning that demonstrate their ability to sufficiently protect the confidentiality of CUI. While automated scanning capabilities are useful tools, they can generate false positives that limited security staff must investigate. Leveraging human professionals to identify vulnerabilities better 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 a properly scoped BBP as an option to help satisfy scanning requirements of Control 3.11.2.

Conclusion

HackerOne thanks NIST 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

[10] NIST, *SP 800-53 Rev. 5*, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[11] NIST, *SP 800-171r3*, Draft, pg. 43, May 2023, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.ipd.pdf.
[12] *Id.*