From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Hacking Policy Council comments
Date: Thursday, July 13, 2023 12:18:47 PM
Attachments: Hacking Policy Council - NIST 800-171 Comment 20230713.pdf
HPC SP800-171r3-ipd-comments .xlsx

Hello.

Please see the attached comments on behalf of the Hacking Policy Council to the draft NIST SP 800-171r3.

Thank you.

Harley Geiger

Harley L. Geiger, Esq. | Venable LLP
[redacted]

[redacted] | www.Venable.com

****
This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.
****

Hacking Policy Council (HPC) Comment Submission for NIST SP 800-171 Rev. 3

Jul. 12, 2023

The Hacking Policy Council ("HPC") submits the following comments in response to the National Institute of Standards and Technology's ("NIST") updated draft guidelines for NIST Special Publication ("SP") 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.[1] We thank NIST for the opportunity to provide input towards improving this essential document.

The HPC is a group of experts dedicated to creating a more favorable legal, policy, and business environment for good faith security research, penetration testing, independent repair for security, and vulnerability disclosure and management.[2] From this perspective, while we are broadly supportive of NIST's approach to updating SP 800-171, the HPC has suggestions that we believe would further strengthen and complete the document.

Add Vulnerability Disclosure Policies

Vulnerability disclosure policies (VDPs) are a key element for the protection of confidentiality of sensitive information in modern cybersecurity programs. We recommend that NIST update control 3.11.2 of SP 800-171 to include VDPs, aligning with the RA-5(11) control in SP 800-53r5.[3]

The confidentiality of sensitive information, such as controlled unclassified information (CUI), is at risk when vulnerabilities are not identified and mitigated. Vulnerabilities are identified through a variety of internal and external sources, some of which are solicited through proactive scanning (i.e., red team exercises), while others are discovered independently from the public at-large. VDPs are a key channel for receiving vulnerability information from independent external sources. There are numerous examples of vulnerabilities affecting information confidentiality that were discovered independently, rather than through an organization's traditional active monitoring process.[4] It is critical that vulnerabilities are reported, regardless of who finds them, so that they can be mitigated to protect the data confidentiality and integrity.[5]

SP 800-171r3's draft control 3.11.2 references active monitoring and scanning as approaches to identify vulnerabilities for mitigation. However, control 3.11.2 is incomplete without referencing VDPs as a channel for receiving information that identifies vulnerabilities from unsolicited or independent sources. This lack of reference to VDPs does not align with acknowledged

[1] NIST, SP 800-171 Rev. 3 (Draft), May 10, 2023, https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft.
[2] Hacking Policy Council, https://hackingpolicycouncil.org.
[3] NIST, SP 800-53 Rev. 5, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[4] See, e.g., Heartbleed. ENISA, Good Practice Guide on Vulnerability Disclosure, Case Studies, Nov. 2015., pg. 32, https://www.enisa.europa.eu/publications/vulnerability-disclosure.
[5] 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.

cybersecurity best practices, including existing NIST guidance, and the HPC strongly encourages ensuring that they are represented.

NIST recognizes the importance of these processes in SP 800-53r5's control RA-5, citing vulnerability disclosure programs and bug bounties as key approaches to vulnerability scanning and monitoring.[6] NIST further underscores the importance of these processes with the inclusion of vulnerability disclosure and handling within the NIST CSF 1.1 subcategory of RS.AN-5,[7] revised in the current CSF 2.0 discussion draft to ID.RA-09.[8] This subcategory calls for the establishment of processes "to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)." Yet these approaches are missing from the draft SP 800-171r3.

Vulnerability disclosure should include information on the development of a VDP, as well as the development of the capabilities to handle vulnerability information that is received. This includes the development of a vulnerability handling process and an organizational framework that addresses organizational roles, responsibilities, and authorities for identifying and verifying vulnerability reports, developing and deploying mitigation measures, and post-mitigation activities.

If SP-800-171 is to be a maximally effective and long-lasting document, NIST should incorporate VDPs in alignment with widely adopted international standards such as ISO/IEC 29147:2018 and ISO/IEC 30111:2019. We suggest referencing SP 800-216 as a supporting document to a revised control 3.11.2 in SP 800-171, as SP 800-216 is aligned with ISO/IEC 29147:2018 and ISO/IEC 30111:2019.[9]

Structure and Formatting

The HPC notes that the current structure of *The Requirements* section places the 17 families of security requirements in alphabetical order. We encourage NIST to consider reordering these families of security requirements into something approaching a pre-incident to post-incident chronology, similar to NIST's reorganization of the categories and subcategories in the recent CSF 2.0 Core discussion draft. Reorganizing in this manner is likely to be more helpful to organizations attempting to understand the role of each family and which other families are closely related to it.

* * *

The HPC thanks NIST for their continued leadership on this issue and for welcoming constructive feedback. We look forward to continuing to work with you to further update and improve SP 800-171.

The Hacking Policy Council

---

[6] NIST, SP 800-53 Rev. 5, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[7] 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.
[8] NIST, Discussion Draft of the NIST Cybersecurity Framework 2.0 Core, 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.
[9] 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.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Hacking Policy Council	General		43	1599	Vulnerability disclosure policies (VDPs) are a key element for the protection of confidentiality of sensitive information in modern cybersecurity programs. The confidentiality of sensitive information, such as controlled unclassified information (CUI), is at risk when vulnerabilities are not identified and mitigated. It is critical that vulnerabilities are reported, regardless of who finds them, so that they can be mitigated to protect the data confidentiality and integrity. VDPs are a key channel for receiving vulnerability information from independent external sources.	The Hacking Policy Council urges NIST to incorporate vulnerability disclosure policies (VDPs) in the revised draft of SP 800-171.
1						SP 800-171r3's draft control 3.11.2 references active monitoring and scanning as approaches to identify vulnerabilities for mitigation. However, control 3.11.2 is incomplete without referencing VDPs as a channel for receiving information that identifies vulnerabilities from unsolicited or independent sources. This lack of reference to VDPs does not align with acknowledged cybersecurity best practices, including existing NIST guidance.	We recommend that NIST update control 3.11.2 of SP 800-171 to include VDPs, aligning with the RA-5(11) control in SP 800-53r5.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1						Vulnerability disclosure should include information on the development of a VDP, as well as the development of the capabilities to handle vulnerability information that is received. This includes the development of a vulnerability handling process and an organizational framework that addresses organizational roles, responsibilities, and authorities for identifying and verifying vulnerability reports, developing and deploying mitigation measures, and post-mitigation activities.	NIST should incorporate VDPs in alignment with widely adopted international standards such as ISO/IEC 29147:2018 and ISO/IEC 30111:2019. We suggest referencing SP 800-216 as a supporting document to a revised control 3.11.2 in SP 800-171. SP 800-216 is aligned with ISO/IEC 29147:2018 and ISO/IEC 30111:2019.
2	Hacking Policy Council	General		vi		The HPC notes that the current structure of The Requirements section places the 17 families of security requirements in alphabetical order. This ordering method is less practical to users than organizing the requirements by role in preventing and responding to incidents.	We encourage NIST to consider reordering the 800-171 security requirements into a pre-incident and post-incident chronology. This would be similar to NIST's reorganization of categories and subcategories in the recent CSF 2.0 Core discussion draft. Reorganizing in this manner will be more useful to organizations attempting to understand the role of each family and which other families are closely related to it.