Joint Response to
National Institute of Standards and Technology
Request for Comment on “NIST Cybersecurity Framework 2.0 Concept Paper”

March 17, 2023

We the undersigned organizations submit these comments in response to the National Institute of Standards and Technology’s (NIST) request for comment on the Cybersecurity Framework (CSF) 2.0 concept paper.[1] Thank you for the opportunity to provide input.

We commend NIST for amending the CSF 1.1 Core in 2018 with subcategory RS.AN-5 on coordinated vulnerability disclosure and handling processes.[2] We support and reiterate previous joint comments to NIST on “Evaluating and Improving NIST Cybersecurity Resources.”[3] As NIST plans the next significant update to the CSF, we urge NIST to

1. Retain the RS.AN-5 subcategory in CSF 2.0; and
2. Include standards directly related to coordinated vulnerability disclosure *in the CSF 2.0 document itself, not just part of online reference tools*. Specifically, ISO/IEC 29147 and 30111 should be included in the informative references to the RS.AN-5 subcategory in the CSF 2.0 document.[4]

We urge NIST to retain RS.AN-5 in CSF 2.0. Modern cybersecurity programs must include processes for receiving, analyzing, and responding to vulnerability disclosures. Increasingly, coordinated vulnerability disclosure and handling processes are incorporated into US and non-US regulations and standards. The RS.AN-5 subcategory is critical to ensure the CSF includes vulnerability disclosure and distinguishes it from other information sharing processes, such as receiving cyber threat intelligence.

We urge NIST to include ISO/IEC 29147 and ISO/IEC 30111 in the informative references for RS.AN-5 in the Framework document. These standards should be included in both the online references NIST contemplates for CSF 2.0, as well as the RS.AN.5 cell in the “informative references” column of the CSF core table. Linking to the online references alone would be insufficient. The online reference tools cited in the CSF 2.0 concept paper - the Cybersecurity and Privacy Reference Tool (CPRT)[5] and the Online Informative References (OLIR) Program[6] - are highly complex to use and may reduce functionality of the Framework for some users. It is also unclear how OLIR would support

[1] NIST, Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework, Jan. 19, 2023, https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf.
[2] National Institute of Standards and Technology, Cybersecurity Framework v1.1, RS.AN-5, Apr. 16, 2018, pg. 42, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[3] Rapid7, Joint Response to National Institute of Standards and Technology Request for Information on “Evaluating and Improving NIST Cybersecurity Resources,” Apr. 25, 2022, Docket ID. NIST-2022-0001, https://www.rapid7.com/globalassets/_pdfs/policy/joint-comments-on-coordinated-vuln-disclosure-in-cybersecurity-framework-apr-24-2022.pdf.
[4] ISO/IEC 29147:2018, Information technology – Security techniques – Vulnerability disclosure, International Standards Organization, Oct. 2018, https://www.iso.org/standard/72311.html. ISO/IEC 30111:2019, Information technology – Security techniques – Vulnerability handling processes, International Standards Organization, Oct. 2019, https://www.iso.org/standard/69725.html.
[5] NIST, Cybersecurity and Privacy Reference Tool, updated Feb. 1, 2023, https://csrc.nist.gov/projects/cprt.
[6] NIST, Online Informative References Program, updated Feb. 14, 2023, https://csrc.nist.gov/projects/olir.

mapping to a single Subcategory. For this reason, it is important to provide the standards in the CSF 2.0 document itself.

Linking to ISO/IEC 29147 and 30111 would provide clarity to all CSF users, including international and small and medium-sized organizations, regarding the best practices for implementing RS.AN-5. To the extent that NIST intends to provide an implementation example for RS.AN-5, we urge NIST to reference ISO/IEC 29147 and 30111 in that example.

The current CSF 1.1 informative references for the RS.AN-5 subcategory do not relate to coordinated vulnerability disclosure, nor do they even mention coordinated vulnerability disclosure, making it more difficult for CSF users to implement the subcategory in conformity with well-established standards. Instead, the current CSF references to COBIT 5, CIS CSC, and NIST SP 800-53 cover more general security risk management activities, which does not provide clarity on the purpose and implementation of RS.AN-5.

By not linking the CSF subcategory on coordinated vulnerability disclosure and handling to ISO/IEC 29147 and 30111, NIST risks falling out of alignment with industry best practices and US and non-US government guidance. For example, ISO/IEC 29147 and ISO/IEC 30111 are directly referenced in the NIST Secure Software Development Framework,[7] the NIST Recommendations for Federal Vulnerability Disclosure Guidelines,[8] the Department of Homeland Security's Binding Operational Directive 20-01,[9] the Department of Justice's framework for vulnerability disclosure programs,[10] the EU's Network and Information Security 2 (NIS 2) Directive,[11] the EU's proposed certification scheme for ICT products,[12] the ENISA guidance on national coordinated vulnerability disclosure policies in the EU,[13] and more.

Organizations looking to implement RS.AN-5 should rely on consistent, internationally-recognized best practices for coordinated vulnerability disclosure. ISO/IEC 29147 and ISO/IEC 30111 are directly applicable to coordinated vulnerability disclosure and handling, and these standards include key guidance that the current CSF v1.1 informative references for RS.AN-5 do not provide. As the US Cybersecurity and Infrastructure Security Agency (CISA) has noted: "International standards ISO 29147 (vulnerability disclosure) and ISO 30111 (vulnerability handling processes) are high quality normative resources. As vulnerability disclosures can come from anyone across the globe, aligning with international best practices can increase shared expectations and minimize the potential for friction."[14]

---

[7] NIST, Secure Software Development Framework, SP 800-218 v1.1, Feb. 2022, pg. 16, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf.
[8] NIST, Recommendations for Federal Vulnerability Disclosure Guidelines, Draft SP 800-216, Jun. 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216-draft.pdf.
[9] Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Binding Operational Directive 20-01, Sep. 2, 2020, https://www.cisa.gov/binding-operational-directive-20-01.
[10] Department of Justice, A Framework for a Vulnerability Disclosure Program for Online Systems, Jul. 2017, pg. 4, https://www.justice.gov/criminal-ccips/page/file/983996/download.
[11] Directive (EU) 2022/2555 of the European Parliament and of the Council, Dec. 4, 2022, Recital 58, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1677267055312&from=en.
[12] ENISA, Cybersecurity Certification: Candidate EUCC Scheme V1.1.1, May 25, 2021, pg. 51, https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1.
[13] ENISA, Coordinated Vulnerability Disclosure Policies In The EU, Apr. 13, 2022, pg. 41, https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu.
[14] Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Binding Operational Directive 20-01, Sep. 2, 2020, https://www.cisa.gov/binding-operational-directive-20-01.

Thank you for your consideration. We look forward to continuing to work with NIST on the next phase of the Cybersecurity Framework.

Sincerely,

Bugcrowd
Business Software Alliance
CERT/Software Engineering Institute
Cyber Policy Working Group
Cybersecurity Coalition
Cyber Threat Alliance
The disclose.io Project
Google
HackerOne
Intel Corp.
Intigriti
Luta Security
NextJenSecurity
Stratigos Security