Joint Response to
National Institute of Standards and Technology Request for Information on “Evaluating and Improving NIST Cybersecurity Resources”

Docket ID. NIST-2022-0001

April 25, 2022

We the undersigned companies, civil society groups, and individuals submit these comments in response to the National Institute of Standards and Technology's (NIST) request for public comment on improving its cybersecurity resources.[1] Thank you for the opportunity to provide input.

We commend NIST for its leadership on developing and advancing the Framework for Improving Critical Infrastructure Cybersecurity (the Cybersecurity Framework), as well as for amending the Framework Core in 2018 with subcategory RS.AN-5 on coordinated vulnerability disclosure and handling processes.[2]

This letter recommends that NIST update the informative references to RS.AN-5 to include standards that are directly related to coordinated vulnerability disclosure - specifically ISO/IEC 29147 and ISO/IEC 30111.[3] Referencing these widely known and adopted international standards on vulnerability disclosure will help drive broad alignment to a common set of best practices and avoid confusion regarding disclosure norms. Presently, the informative references for RS.AN-5 are not directly related to coordinated vulnerability disclosure and handling.

---

[1] 87 FR 9579, National Institute of Standards and Technology, Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, Feb. 22, 2022, https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity.

[2] National Institute of Standards and Technology, Cybersecurity Framework Version 1.1, RS.AN-5, Apr. 18, 2018, pg. 42, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. See also, Joint Comments on "Framework for Improving Critical Infrastructure Cybersecurity" version 1.1, Apr. 10, 2017, https://www.rapid7.com/globalassets/_pdfs/rapid7-comments/joint-comments-to-nist-framework-revision-1.1---rapid7---041017.pdf.

[3] 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.

Processes for receiving, reviewing, handling, and responding to vulnerability disclosures are a core component of modern cybersecurity programs.[4] The RS.AN-5 subcategory effectively incorporates these processes and distinguishes them from other formal information sharing arrangements (such as receiving cyber threat intelligence from information sharing forums, as described in ID.RA-2). We support retaining the RS.AN-5 language in the Cybersecurity Framework, and also support retaining the discussion of coordinated vulnerability disclosure in the NIST Roadmap.[5]

However, the informative references to RS.AN-5 currently listed in the Cybersecurity Framework V1.1 do not directly relate to, or even mention, coordinated vulnerability disclosure and handling processes. The current references to COBIT 5 and CIS CSC cover broadly applicable risk management, system monitoring, and incident response activities.[6] The current references to NIST SP 800-53 cover security advisories and testing/training/monitoring activities in general.[7] The use of these informative references makes it more difficult for Cybersecurity Framework users to link RS.AN-5 with well-established coordinated vulnerability disclosure and handling practices.

By contrast, ISO/IEC 29147 and 30111 are directly applicable to coordinated vulnerability disclosure and handling processes. These complementary standards encompass important nuances that are not fully covered by the current RS.AN-5 informative references, such as strengthening internal mechanisms for dealing with received reports, interfacing with the party disclosing vulnerability information, and more. As coordinated vulnerability disclosure and handling processes are more widely adopted, organizations rely on detailed guidance from a consistent set of internationally recognized best practices to avoid conflicting processes that can undermine security. This is particularly important given the global nature of these processes.

---

[4] Establishing a coordinated vulnerability disclosure and handling process – and communicating the existence and scope of that policy publicly – can help organizations quickly detect and respond to vulnerabilities disclosed to them by a variety of sources, leading to mitigations that enhance the security, data privacy, and safety of their systems.

[5] The Roadmap refers to ISO/IEC 29147 and 30111, though the Cybersecurity Framework itself does not. NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, Apr. 25, 2019, pg. 9, https://www.nist.gov/system/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf.

[6] ISACA, COBIT 5 Framework, EDM03.02 and DSS05.07, https://www.isaca.org/resources/cobit/cobit-5. Center for Internet Security, Critical Security Controls, 4 and 19, https://www.cisecurity.org/controls (last accessed Mar. 31, 2022).

[7] NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, SI-5 and PM-15, pgs. F-224 and G-9,
Apr. 30, 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

The absence of more direct references risks putting the 2018 Cybersecurity Framework out of sync with other key guidance on coordinated disclosure and handling from government and the private sector. For example, ISO/IEC 29147 and ISO/IEC 30111 are directly referenced in the CERT Guide to Coordinated Vulnerability Disclosure,[8] the Department of Homeland Security's Binding Operational Directive 20-01,[9] the IoT Cybersecurity Improvement Act of 2020, [10] the Department of Justice's framework for vulnerability disclosure programs for online systems,[11] the Food and Drug Administration's postmarket guidance for cybersecurity in medical devices,[12] the EU's proposed certification scheme for ICT products,[13] the EU's proposed Network and Information Security Directive (NIS 2),[14] and elsewhere.

Accordingly, with the goal of helping Cybersecurity Framework users develop coordinated disclosure and handling processes consistent with best practices and international standards, we request that NIST incorporate ISO/IEC 29147 and 30111 as informative references to RS.AN-5.

Thank you for your consideration. We look forward to working with NIST to further optimize the Cybersecurity Framework.

---

[8] "Readers are encouraged to review and apply those standards to their operational vulnerability response practice." Householder et al., The CERT Guide toCoordinated Vulnerability Disclosure, Aug. 2017, pg. 18, https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

[9] "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." 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. See also NIST's draft Vulnerability Disclosure Guidance, NIST SP 800-216 (Draft), Recommendations for Federal Vulnerability Disclosure Guidelines, Jun. 7, 2021, https://csrc.nist.gov/Projects/vdg/publications.

[10] Pub. Law 116-207, 116th Cong., Sec. 5(b)(1).

[11] 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.

[12] "FDA has recognized ISO/IEC 29147:2014 [...] and ISO/IEC 30111:2013 [...] that may be useful resources for manufacturers." Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Dec. 28, 2016, pgs. 13, 28, https://www.fda.gov/media/95862/download.

[13] "Previously undetected vulnerability shall be reported and handled in accordance with the general rules of ISO/IEC 30111 and ISO/IEC 29147[...]" 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.

[14] See European Commission, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, Document 52020PC0823, Recital 28, Dec. 16, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0823.

Sincerely,

Companies & groups:

Rapid7
Access Now
Bugcrowd
Business Software Alliance (BSA)
Center for Democracy & Technology (CDT)
Cisco
Cybereason
Cybersecurity Coalition
Cybersecurity Policy Working Group (CPWG)
Cyber Threat Alliance
disclose.io Project
Electronic Frontier Foundation (EFF)
Google
HackerOne
IBM X-Force
Information Technology Industry Council (ITI)
Intel
Luta Security
New America's Open Technology Institute
Palo Alto Networks
Red Hat, Inc.
SCYTHE, Inc.
Trellix

Individuals:
(Institutional affiliation for identification purposes only.)

Casey Ellis, Pioneer of Crowdsourced Security as-a-Service
Art Manion, CERT Coordination Center, co-editor of ISO 29147 & ISO 30111
Katie Moussouris, Founder and CEO, Luta Security, co-editor of ISO 29147 & ISO 30111