

**Joint Comments on
"Framework for Improving Critical Infrastructure Cybersecurity"
Version 1.1 Draft 2
Before the National Institute of Standards and Technology**

Jan. 19, 2018

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 Version 1.1 Draft 2 of the "Framework for Improving Critical Infrastructure Cybersecurity " (the "Framework").¹

We commend NIST for their leadership on developing and advancing the Framework, as well as for its addition of a subcategory (RS.AN-5) relating to coordinated vulnerability disclosure and handling processes to the Framework Core.²

We urge the retention of RS.AN-5 in the final version of the Framework. We also urge NIST to list standards that are directly relevant to coordinated vulnerability disclosure as informative references for RS.AN-5.

The Framework should retain coordinated vulnerability disclosure and handling processes

Processes for receiving, reviewing, and responding to vulnerability disclosures should be considered a core component of modern cybersecurity plans.³ We recommend that the final version of the Framework retain the proposed RS.AN-5 subcategory language in order to help organizations evaluate their preparedness to respond to vulnerability disclosures from internal and external sources. Similarly, we also support retaining the discussion of coordinated

¹ National Institute of Standards and Technology, Cybersecurity Framework Version 1.1 Draft 2, Request for public comments, <https://www.nist.gov/cyberframework/draft-version-11> (last accessed Jan. 19, 2017).

² National Institute of Standards and Technology, Cybersecurity Framework Version 1.1 Draft 2, RS.AN-5, Dec. 5, 2017, pg. 49, https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_with-markup.pdf.

³ See discussion in joint comments to NIST Framework version 1.1 Draft 1, pgs. 1-3, Apr. 10, 2017, <https://www.nist.gov/sites/default/files/documents/2017/05/12/2017-04-10-consortium.pdf>. Vulnerability disclosure and handling processes are formal internal mechanisms for receiving, assessing, and mitigating security vulnerabilities submitted by external sources, such as independent researchers acting in good faith, and communicating the outcome to the vulnerability reporter and affected parties. Such processes do not apply to a vendor's products and services alone. Organizations should be prepared to receive disclosures regarding vulnerabilities in their infrastructure and system configuration as well. If an organization receives a vulnerability that actually applies to another vendor's products, the organization should nonetheless have a process for receiving the vulnerability and passing it on to the appropriate vendor. Organizations may receive threat intelligence information from formal information sharing arrangements, such as coordination with Information Sharing and Analysis Centers, but organizations are likely to receive additional (potentially unsolicited) disclosures from external sources independent of those arrangements. Coordinated vulnerability disclosure and handling processes may or may not actually incentivize searching for vulnerabilities (such as by offering bounties for bug submissions) or provide a guarantee of legal liability protection. Organizations will need to determine for themselves whether offering incentives for disclosures is the best fit for them.

vulnerability disclosure in the NIST Roadmap draft version 1.1.⁴

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 external sources, leading to mitigations that enhance the security, data privacy, and safety of their systems.⁵ Vulnerability disclosure and handling processes can also help protect researchers or accidental discoverers acting in good faith by providing them with a clear channel to communicate vulnerabilities to technology providers and operators, reducing the risk of conflict or misunderstanding.

Earlier versions of the Framework included information sharing and external participation, but the proposed RS.AN-5 language provides additional clarity. This subcategory is more explicit that organizations should be prepared to receive and respond to vulnerability disclosures from a spectrum of sources, including unsolicited disclosures from researchers. The proposed RS.AN-5 helps distinguish this process from other types of information sharing, such as (for example) receiving cyber threat intel from information sharing forums and sources in ID.RA-2.

The Framework should incorporate informative references directly related to coordinated disclosure and handling processes

Best practices for vulnerability disclosure and handling processes are available through the ISO 29147 and 30111 standards.⁶ We recommend that the Framework itself list both of these standards as an informative reference to RS.AN-5.

The Roadmap draft references both standards and expressly notes that coordinated vulnerability disclosure and handling processes are included in the Framework draft.⁷ However, the Framework draft itself does not reference these standards. Listing ISO 29147 and 30111 as informative references to RS.AN-5 would help clarify to users – from the text of the Framework itself, rather than the Roadmap alone – that the subcategory covers coordinated vulnerability disclosure, and help users develop processes that accommodate a variety of coordinated disclosure situations. If the Framework excludes these standards and keeps only its current list, there is greater risk that users may conflate coordinated vulnerability disclosure with other incident management activities.

The informative references to RS.AN-5 currently listed in the draft Framework, though helpful, do not provide an adequate level of relevant detail on coordinated vulnerability disclosure and handling processes. For example, references to NIST SP 800-53 cover security advisories and

⁴ Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, Dec. 5, 2017, pg. 5, https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf.

⁵ See, e.g., Matthew Finifter et al., An Empirical Study of Vulnerability Rewards Programs, 22nd Usenix Security Symposium, Aug. 14, 2013, https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf.

⁶ ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling, International Standards Organization, Nov. 1, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231. ISO/IEC 29147:2014, Information Technology – Security Techniques – Vulnerability Disclosure, International Standards Organization, Feb. 15, 2014, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170.

⁷ Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, Dec. 5, 2017, pg. 5.

testing/training/monitoring activities in general.⁸ The COBIT 5 and CIS references cover broadly applicable risk management, system monitoring, and incident response activities.⁹ By contrast, ISO 29147 and 30111 are directly applicable to coordinated vulnerability disclosure and handling processes. The two standards are complementary and cover these particular processes from multiple facets, such as strengthening internal mechanisms for dealing with received disclosures, interfacing with the party disclosing vulnerability information, and more.¹⁰ ISO 29147 is freely available to the public.¹¹

*

*

*

We appreciate the opportunity to share our views. Thank you for your consideration. We look forward to working with NIST to further optimize the Framework.

Sincerely,

Rapid7
 Access Now
 Bugcrowd
 Center for Democracy & Technology
 Cisco
 Coalition for Cybersecurity Policy and Law
 Cybereason
 Duo Security
 Electronic Frontier Foundation
 GRIMM
 HackerOne
 I Am The Cavalry
 Kenna Security
 Luta Security
 McAfee
 New America's Open Technology Institute
 Niskanen Center
 Symantec
 TechFreedom

Art Manion, CERT Coordination Center
 Katie Moussouris, Founder and CEO, Luta Security, co-editor of ISO 29147 Vulnerability disclosure & ISO 30111 Vulnerability handling processes
 Nicholas Percoco, Founder of THOTCON
 C.Thomas (Space Rogue), Security Researcher, IBM

⁸ NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, SI-5 and PM-15, pgs. F-188 and G-7, Apr. 30, 2013, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

⁹ ISACA, COBIT 5 Framework, EDM03.02 and DSS05.07, <http://www.isaca.org/COBIT/Pages/Product-Family.aspx> (last accessed Jan. 19, 2018). Center for Internet Security, Critical Security Controls, 4 and 19, <https://www.cisecurity.org/controls> (last accessed Jan. 19, 2018).

¹⁰ See discussion of interplay at ISO/IEC 29147:2014, pgs. 3-4.

¹¹ International Organization for Standardization, Freely Available Standards, <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html> (last accessed Jan. 19, 2018).