From: Harley Geiger
Date: Monday, April 10, 2017 at 9:57 AM
To: <cyberframework@nist.gov>
Subject: Joint comments to NIST Framework revision 1.1

Hello.

Please find attached joint comments to the Cybersecurity Framework draft version 1.1. The comments recommend that the Framework expressly incorporate coordinated vulnerability disclosure and handling processes.

The comments are signed by

Rapid7
Access Now
Bugcrowd
Center for Democracy & Technology
Cisco Systems, Inc.
Cybereason
Duo Security
Electronic Frontier Foundation
Grimm Security
HackerOne
I Am The Cavalry
Luta Security
New America's Open Technology Institute
Niskanen Center
Online Trust Alliance
Security of Things Forum
Symantec
TechFreedom
Tenable
WhiteScope

Brian Knopf, Senior Director of Security Research & IoT Architect, Neustar
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

Please contact me if you have any questions. Thank you very much.

_
Harley Geiger
Director of Public Policy
Rapid7

[Attachment Copied Below]

Joint Comments on "Framework for Improving Critical Infrastructure Cybersecurity" version 1.1 Before the National Institute of Standards and Technology

Apr. 10, 2017

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 of the "Framework for Improving Critical Infrastructure Cybersecurity " (the "Framework").[1] We commend NIST for their leadership on developing and advancing the Framework, and support the Framework's role in helping organizations strengthen their cybersecurity practices.

In its revisions to the Cybersecurity Framework, we recommend that NIST explicitly incorporate *coordinated vulnerability disclosure and handling processes* into the Framework Core and Tiers. Building such processes into the Framework would not be a major revision, but rather a clarification of existing elements of the Framework that will help organizations evaluate their preparedness to respond to vulnerability information and communicate with internal and external stakeholders.

Vulnerability disclosure and handling processes strengthen security programs

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.[2] 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 disclosures from external sources independent of those arrangements.

Recognizing that there is no perfect security and that all vulnerabilities cannot be completely eliminated from digital goods and services pre-market, organizations must be prepared to continually identify and respond to cybersecurity flaws in their infrastructure and networks throughout the IT lifecycle. Yet the quantity, diversity, and complexity of vulnerabilities will prevent many organizations from detecting all vulnerabilities without independent expertise or

[1] National Institute of Standards and Technology, Cybersecurity Framework Draft Version 1.1, Request for public comments, https://www.nist.gov/cyberframework/draft-version-11 (last accessed Apr. 9, 2017).

[2] Note, such processes are not necessarily "bug bounty programs" and may not offer incentives to vulnerability reporters. Bug bounty programs are a subset of coordinated vulnerability disclosure and handling processes. Organizations will need to determine for themselves whether offering incentives for disclosures is the best fit for them.

manpower.[3] This may be especially true for organizations with limited experience or resources for cybersecurity. To catch vulnerabilities they might otherwise overlook, businesses and government agencies are increasingly implementing vulnerability disclosure and handling processes, but adoption of flexible and mature processes for handling unsolicited vulnerability reports is not yet the norm.[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. Such processes should be voluntary and 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.

Best practices for vulnerability disclosure and handling processes are available through, among other sources, the ISO 29147 and 30111 standards.[6] Multiple resources on implementing vulnerability disclosure and handling processes are also available, including through the National Telecommunications and Information Administration's multistakeholder process.[7] These standards and guides are useful roadmaps, but each organization may tailor the process to meet its unique business model, technology, context, and resources.

[3] In fulfilling Framework Core subcategory ID.RA-1, most organizations are unlikely to find all asset vulnerabilities on their own and will leverage information about discovered vulnerabilities provided by vendors, providers, researchers, or other external sources.

[4] *See* I Am The Cavalry, US Government Coordinated Disclosure, Dec. 2016, https://www.iamthecavalry.org/usgdisclosure. *See also* Federal Trade Commission, Federal Trade Commission Public Comment on NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template", Feb. 15, 2017, pgs. 1-2, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-commentnational-telecommunications-information-administration-regarding-safety-working/170215ntiacomment.pdf. *See also* Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff, Dec. 28, 2016, pg. 14, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. *See also* Sean Gallagher, *GM embraces white-hat hackers with public vulnerability disclosure program*, Ars Technica, Jan. 8, 2016, http://arstechnica.com/security/2016/01/gm-embraces-white-hats-with-public-vulnerabilitydisclosure-program.

[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. " "We find that vulnerability reward programs (VRPs) appear to provide an economically efficient mechanism for finding vulnerabilities, with a reasonable cost/benefit trade-off[.] In particular, they appear to be 2-100 times more cost-effective than hiring expert security researchers to find vulnerabilities."

[6] *See* 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. *See also* 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] National Telecommunications and Information Administration, "Early Stage" Coordinated Vulnerability Disclosure Template Version 1.11, NTIA Safety Working Group, Dec. 15, 2016, https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf. *See also*, Katie Moussouris, A Maturity Model for Vulnerability Coordination, HackerOne, Sep. 22, 2015, https://www.hackerone.com/blog/vulnerability-coordination-maturity-model.

The Framework should incorporate coordinated vulnerability disclosure and handling processes

Processes for receiving, reviewing, and responding to vulnerability disclosures should be considered a basic, and relatively easily achievable, component of modern cybersecurity plans. The Framework already provides for information sharing and external participation, but we believe the Framework should be more explicit that these functions encompass coordinated vulnerability disclosure and handling processes.

Framework Core:

The clearest way to incorporate coordinated vulnerability disclosure and handling processes into the Framework Core would be to include a new subcategory dedicated to this concept. For example, NIST could add a subcategory to Risk Assessment (ID.RA) – "*ID.RA-7: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from external sources*" – and cite ISO/IEC 30111:2013 and ISO/IEC 29147:2014 as "informative references."

In addition, the Framework Core could incorporate coordinated vulnerability disclosure and handling processes by clarifying the scope of existing subcategories. For example:

- The "identify" function, at ID.RA-2, urges organizations to receive cyber threat intelligence and vulnerability information from "information sharing forums and sources."[8] The Framework should make clear that "The organization is prepared to receive and analyze cyber threat intelligence and vulnerability information from information sharing forums *or any other external source*" (such as security researchers or accidental discoverers), not just information sharing sources with which the organization may have a formal arrangement (such as ISACs or ISAOs). ID.RA-2 could also cite ISO/IEC 30111:2013 and ISO/IEC 29147:2014 as informative references.

- The "protect" function, at PR.AT-3, includes awareness and training so that third party stakeholders understand roles and responsibilities.[9] This should expressly encompass third parties that submit vulnerabilities to the organization, but who have no formal relationship to the organization (e.g., "suppliers, customers, partners, or *unaffiliated parties that submit vulnerability information, etc.*"). Organizations should aim to make such third parties aware of (or able to easily find) desired communication channels, such as a public facing email address dedicated to receiving vulnerability disclosures, and any applicable security policies. As above, PR.AT-3 could list ISO/IEC 30111:2013 and ISO/IEC 29147:2014 as "informative references."

[8] National Institute of Standards and Technology, Cybersecurity Framework Draft Version 1.1, Framework Tiers, ID.RA-2, Jan. 10, 2017, pg. 29, https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurityframework-v1.1-with-markup.pdf.

[9] *Id*., at PR.AT-3, pg. 33.

Framework Tiers:

The "external participation" metric of the Framework Tiers should be fleshed out to address the maturity of an organization's coordinated vulnerability disclosure and handling processes.[10] This will help align the external participation metric with a revised ID.RA-2, and reinforce that organizations should be prepared to handle vulnerability disclosures from unaffiliated third parties. Below, in italics, is suggested language as a starting point for discussion:

- **Tier 1: Partial,** External Participation – An organization may not have the processes in place to participate in coordination or collaboration with other entities. *The organization has a public-facing channel for receiving vulnerability disclosures from external sources, but these disclosures are handled in an ad hoc manner*.

- **Tier 2: Risk Informed**, External Participation – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally. *The organization has a public-facing channel dedicated to receiving vulnerability disclosures from external sources, and has an internal triage process for reviewing disclosures.*

- **Tier 3: Repeatable**, External Participation – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events. *The organization has a public-facing channel dedicated to receiving vulnerability disclosures from external sources, and has internal processes for reviewing disclosed vulnerabilities, tracking disclosed vulnerabilities to resolution, and distributing critical advisories as necessary.*

- **Tier 4: Adaptive**, External Participation – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs. *The organization has a public-facing channel dedicated to receiving vulnerability disclosures from external sources, and has dedicated resources for reviewing, tracking, and mitigating disclosed vulnerabilities; the organization coordinates communications about the disclosure process and disclosed vulnerabilities with the original vulnerability reporter, partners, customers, the public, and other external stakeholders, as appropriate.*

[10] *See*, e.g., Katie Moussouris, Vulnerability Coordination Maturity Model, HackerOne, Sep. 22n 2015, https://hackerone.box.com/shared/static/77z16vdt5micjd83fj94s3d30dumf8jr.pdf.

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

Sincerely,

Rapid7
Access Now
Bugcrowd
Center for Democracy & Technology
Cisco Systems, Inc.
Cybereason
Duo Security
Electronic Frontier Foundation
Grimm Security
HackerOne
I Am The Cavalry
Luta Security
New America's Open Technology Institute
Niskanen Center
Online Trust Alliance
Security of Things Forum
Symantec
TechFreedom
Tenable
WhiteScope

Brian Knopf, Senior Director of Security Research & IoT Architect, Neustar
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