From: **Harley Geiger**
Date: Mon, Apr 10, 2017 at 12:50 PM
Subject: Rapid7 comments to NIST Framework revision 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: "Witte, Gregory

Hello.

Please find attached Rapid7's comments to the Cybersecurity Framework draft version 1.1. The comments recommend 1) Use of the Framework beyond critical infrastructure, 2) Accounting for credential-based attacks with user behavior analytics and multi-factor authentication, 3) Embedding security in the systems development life cycle, and 4) Preparing coordinated vulnerability disclosure and handling processes.

Please note the attached comments are separate from the joint comments we submitted earlier today. The attached comments are from Rapid7 only. The joint comments were on behalf of a broader coalition.

Please let me know if you have any questions. Thank you very much.

_
Harley Geiger
Director of Public Policy
Rapid7

[Attachment Copied Below]

Comments on "Framework for Improving Critical Infrastructure Cybersecurity" version 1.1

Before the National Institute of Standards and Technology

Apr. 10, 2017

Rapid7 submits 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.

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cyber security. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks.

Use of the Framework beyond critical infrastructure

Rapid7 supports use of the Framework beyond critical infrastructure, ideally as a guide for organizations of many types to enhance their security postures. In the time since the Framework was released, it has gained a reputation of credibility and already seen impressive adoption both among critical infrastructure and non-critical infrastructure organizations. We believe the Framework should acknowledge this usage by expressly expanding the applicability of the Framework beyond critical infrastructure. Because business, personal, and government networks are all increasingly closely linked, strengthening the cybersecurity of such organizations will also serve to strengthen critical infrastructure. We recommend NIST work with the Administration to explore how the Framework can be revised to expressly apply to non-critical infrastructure organizations.[2]

Accounting for credential-based attacks – user behavior analytics and strong authentication

Since the initial development of the Framework, it has become increasingly well-established that theft and malicious use of user credentials play a part in a large volume of security breaches.[3] According

---

[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] This may require updates to Executive Order 13636, Sec. 7, 78 FR 11741, Feb. 12, 2013, https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

[3] Verizon 2016 Data Breach Investigations Report, Apr. 2016, pg. 20, http://www.verizonenterprise.com/verizon-insightslab/dbir/2016.

to the 2016 Verizon Data Breach Report, 63% of data breaches involved weak, default or stolen passwords. The Commission on Enhancing the National Cybersecurity also underscored this development in its 2016 report: "A review of major breaches over the past six years reveals that compromised identity characteristics have consistently been the main point of entry."[4] To reflect this trend and better prepare organizations against this serious attack vector, the Framework should clearly include processes that counter the risks of stolen or misused credentials.

We recommend NIST clarify Framework Core functions to include Processes that account for misuse of legitimate user credentials or assets, such as user behavior analytics. We believe this concept should be an express part of the Core because the seriousness and prevalence of the threat make some level of behavior monitoring a fundamental protection. The Framework Core "detect" function – at DE.CM-3 – indicates that personnel activity should be monitored for cybersecurity events. We suggest the following revision in italics: "DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events, *including loss or misuse of user credentials or assets."* Informative references could include the CERT Insider Threat Best Practices.[5]

In addition, we recommend NIST incorporate multi-factor authentication into the Framework Tiers' "Integrated Risk Management Program" metric.[6] Although we view multi-factor authentication as a key protection measure, we suggest use of the Tiers rather than the Core to provide additional flexibility for organizations – while all organizations should manage credentials under the PR.AC category, multi-factor authentication should at least be deployed by organizations with mature and rigorous risk management programs. Accordingly, we suggest revising the Tier 3 metric to include the following: "*User access to critical systems is protected with strong or multi-factor authentication.*" We also suggest revising the Tier 4 metric to include the following: "*The organization deploys strong or multi-factor authentication widely to prevent unauthorized access to sensitive data.*"

Embedding security in the systems throughout the development life cycle

We support the Framework Core's inclusion of the systems development life cycle to manage systems in PR.IP-2. However, the subcategory does not indicate the role security should play in the life cycle. Embedding security principles and testing in from the start, at the planning and design stages of the process, is significantly more effective than retrofitting security in the later stages. As a cybersecurity guide, we suggest that the Framework should emphasize the role of security in the whole life cycle rather than just recommend the use of the life cycle. We suggest modifying PR.IP-2 with the italicized language "A Systems Development Life Cycle to manage systems is implemented, *prioritizing security testing throughout the life cycle.*"

---

[4] Commission on Enhancing the National Cybersecurity, Dec. 1, 2016, pg. 17, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[5] Silowash et al., Common Sense Guide to Mitigating Insider Threats, 4th Edition, Dec. 2012, https://www.cert.org/insiderthreat/best-practices.

[6] National Institute of Standards and Technology, Cybersecurity Framework Draft Version 1.1, Jan. 10, 2017, pgs. 9-12, https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf.

Preparing coordinated vulnerability disclosure and handling processes

Rapid7 urges NIST to incorporate coordinated vulnerability disclosure and handling processes into the Framework Core and Tiers. We support the recommendations submitted in joint comments to NIST by a coalition of companies, civil society groups, and individuals during this comment cycle.[7]

* * *

We appreciate the opportunity to share our views. If there are additional questions or if Rapid7 can provide any further assistance, please contact Harley Geiger, Director of Public Policy.
Thank you.

END

---

[7] Rapid7 et al., Joint Comments on "Framework for Improving Critical Infrastructure Cybersecurity version 1.1, Before the National Institute of Standards and Technology, Apr. 10, 2017, https://rapid7.com/globalassets/_pdfs/rapid7-comments/joint-comments-to-nist-framework-revision-1.1---rapid7---041017.pdf.