April 25, 2022

Submitted via email to CSF-SCRM-RFI@nist.gov

Cybersecurity Framework
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Subject: RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Tenable®, Inc. (Tenable) appreciates the opportunity to provide comments on the National Institute of Standards and Technology (NIST) Request for Information on evaluating and improving cybersecurity resources, including the Framework for Improving Critical Infrastructure Cybersecurity (Framework).

Tenable is the Cyber Exposure company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at tenable.com.

Tenable has provided comments regarding the usefulness of the Framework for cybersecurity risk management, recommendations for developing additional resources, such as maturity levels and benchmark metrics to help more organizations adopt the Framework, and recommendations for specific updates to the Framework Core to better reflect current risk management best practices.

Usefulness of the Framework

Tenable believes the Framework is a useful tool for aiding organizations in cybersecurity efforts, and that the five functions and corresponding categories and subcategories are easily understood and communicated within and between organizations. Tenable uses a combination of ISO 27001 and the Framework to manage and measure our cybersecurity program. We use the Framework as an overall framework for our cybersecurity program and to measure maturity and track progress. We use ISO 27001 for the management of our cybersecurity program but not to measure maturity.

Additional Resources to Support Framework Adoption

The Framework necessitates a certain level of maturity and appropriate resources for an organization to be able to map its cybersecurity activities to the respective subcategories within the five functions. Organizations which have reached a certain level of maturity, and which have adequate resources and budget, require considerable time and effort to align their cybersecurity practices to the Framework.

Maturity levels, similar to Center for Internet Security Controls Implementation Groups, would be helpful resources for organizations either lacking maturity to fully adopt the Framework or for those that are seeking to align practices with the Framework for the first time. In addition, anonymized sector-specific benchmarking metrics would be valuable for organizations that are seeking to adopt the Framework by helping them measure their progress against industry peers with similar profiles and risk/threat environments.

Tenable does not believe NIST should make significant structural changes (Functions / Categories / Subcategories) to the Framework. However, should the structure of the Framework change, NIST should provide a reverse mapping of Functions / Categories / Subcategories to help organizations transition from one version to the next.

Relationship of the Framework to Other Risk Management Resources

Tenable supports greater Framework alignment and interoperability with the Secure Software Development Framework (SSDF). In addition, the Framework would benefit from incorporation of cloud security best practices into the Framework Core. Alignment with cloud specific frameworks such as CSA Star v4 would be useful. While the Risk Management Framework (RMF) is useful for certain regulated industries, the RMF is too intensive for the majority of private sector businesses and organizations. Finally, Tenable would recommend a clearly aligned mapping of the Framework to the newest version of ISO 27002, Information Security Controls, which has recently been published.

Recommended Changes to the Framework Core

Tenable recommends the following changes to Framework Core Subcategories to reflect the expanded attack surface, evolved vulnerability management practices, continuous assessment of authorizations, attack path analysis, and implementation metrics.

Enterprise attack surfaces are growing in complexity and cyber criminals are deploying more advanced methods to target user and enterprise infrastructure weaknesses. Today's modern network environment goes beyond the scope of traditional IT- to include cloud, OT, mobile and web apps. Different types of assets constantly enter and exit the enterprise. NIST should incorporate changes to the Framework Core to address cyber risk management associated with connected assets across IT, IoT, OT, mobile, container, and cloud environments.

Tenable also recommends that NIST strengthen Framework subcategories on vulnerability management to ensure that organizations focus on mitigating and/or remediating vulnerabilities that pose the greatest threat based on factors such as severity, exploitability, and asset criticality. This is consistent with both guidance from version 3.1 of the Common Vulnerability Scoring System[1] as well as the Stakeholder Specific Vulnerability Categorization practices developed by the Software Engineering Institute and employed by the Cybersecurity and Infrastructure Security Agency (CISA)[2].

[1] https://www.first.org/cvss/v3.1/user-guide
[2] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379

Enterprises and organizations rely on software like Active Directory and other means to provision users, roles, and access. With most breaches involving the theft of user identity and credentials, Active Directory is a fundamental tool and is therefore a frequent target of bad actors. If identity systems are compromised, attackers can escalate privileges and move laterally throughout the network. Unfortunately, many organizations conduct infrequent, manual audits of these access management systems. NIST should incorporate continuous assessments of access permissions and authorizations into the Framework Core to address this challenge.

Proposed Framework Core changes are in red:

ID.AM-1: Physical devices and systems, including IT, Operational Technology, Internet of Things, mobile, and cloud environments, within the organization are inventoried and prioritized by criticality

ID.RA-1: Asset vulnerabilities are identified and documented and prioritized by likelihood of exploitation

ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources and incorporated into prioritization efforts

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used both to determine risk and prioritize remediation efforts (see also DE.CM-8 below)

ID.RA-6: Risk responses are identified and prioritized and remediation efforts are tracked

PR.AC-4: Access permissions and authorizations are managed and continuously assessed, incorporating the principles of least privilege and separation of duties

PR.IP-12: A vulnerability management plan, prioritizing mitigation of vulnerabilities that pose the greatest threats based on factors such as severity, exploitability and asset criticality, is developed and implemented and vulnerability remediation efforts are tracked

DE.AE-2: Detected events are analyzed to understand attack targets and methods; attack paths are identified and remediation efforts implemented

DE.CM-8: Vulnerability scans are performed and the frequency, depth and comparative performance benchmarks are measured and communicated to relevant stakeholders

RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) and remediation efforts are prioritized based on criticality of assets and likelihood of vulnerability being exploited

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks and prioritized by criticality of asset and risk of vulnerability being exploited

Thank you for the opportunity to provide comments and feedback with regards to evaluation and improvement of NIST cybersecurity resources, including updates to the NIST Cybersecurity Framework. Tenable is committed to supporting NIST and our U.S. government partners as we drive to improve critical infrastructure cybersecurity. If you have any questions about our submission, please contact Jamie Brown, Sr. Director, Global Government Affairs, at [redacted]