Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

November 5, 2023

Emailed to cyberframework@nist.gov

National Institute of Standards and Technology (NIST)

United States Department of Commerce

100 Bureau Drive

Gaithersburg, MD 20899

Subject: Microsoft Comments on the Public Draft: The NIST Cybersecurity Framework 2.0

Introduction

Microsoft welcomes the opportunity to provide comments on the request for information (RFI) for the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF 2.0). As a provider of technology products and services to more than one billion customers in the United States and worldwide, Microsoft is constantly innovating and investing in developing, maturing, and promoting cybersecurity best practices both internally across our company and externally with our ecosystem of security partners and customers. This ongoing commitment to improving our collective digital defense allows Microsoft to provide unique and valuable insights to NIST with the goal of strengthening the RFI.

Microsoft believes the current public draft NIST CSF 2.0 responds to the primary cybersecurity concerns across the ecosystem and addresses many of the needs expressed by the cybersecurity stakeholders while still maintaining the Framework's flexibility, interoperability, and technology neutrality for a broad audience. We support major NIST CSF 2.0 changes including:1) adding a GOVERN function; 2) raising supply chain risk management at the governance level while addressing it holistically across the Framework; 3) developing practical guidance for practitioners such as implementation examples and 4) clarifying profiles, tiers, and offering greater alignment of the CSF 2.0 with other NIST resources.

In this final stage of the CSF 2.0 development process, we offer additional adjustments and future-oriented recommendations that focus on improving guidance, resources, and tools to drive greater adoption and effective implementation across the global CSF 2.0 ecosystem.

Recommendations

I. Collaborate with international standards bodies to strengthen the global cybersecurity ecosystem and foster global adoption

While NIST has made substantial efforts to brand the Framework, including multiple translations into foreign languages and international outreach and engagement to promote it as an international framework, the international community still perceives it as a US-centric framework. To broaden the adoption of the NIST CSF 2.0, it is important that NIST leverages the ISO/IEC standards development process to foster global adoption of the NIST CSF 2.0. To this end, we encourage NIST to continue aligning with the ISO/IEC 27000 series. This includes ongoing integration of ISO/IEC 27001 as an Informative Reference and updating ISO/IEC 27103 and ISO/IEC 27110 to ensure compatibility and alignment with CSF 2.0. Because those derivative approaches rest on a common security baseline of practices -- as well as a common taxonomy and lexicon -- organizations can build and maintain cyber risk management approaches which work across borders and industries. Microsoft supports NIST's efforts to grow and strengthen the inventory of informative references for use with CSF 2.0. This will drive alignment across global cybersecurity risk management efforts with other international risk-based standards, such as ISO and IEC standards. We support using National Online Informative References (OLIR) to clarify relationships with international cybersecurity standards such as ISO/IEC 27103, ISO/IEC 29147, and ISO/IEC 30111.

II. Develop best practices for creating Community Profiles to foster consistency and increase global use and adoption

Microsoft commends NIST for providing new, practical guidance in CSF 2.0 for using Framework Profiles to increase global adoption. Including the definition for Community Profile along with guidance for creating this Profile and specific examples is extremely valuable for practitioners. However, we believe there is an opportunity to further promote the use of Community Profiles by providing guidance and best practices for organizations aiming to collaborate in the creation of Community Profiles for a sector or subsector.

In our April 2022 and March 2023 comments to NIST, we recommended a cross-sector cloud security profile or cloud extension be created with the goal of providing more resources for securing cloud deployments and we welcome the opportunity to work collaboratively with NIST and industry bodies to facilitate this effort. There is increasing interest in Community Profiles for critical infrastructure sectors, with some efforts already underway, and we believe a cross-sector cloud security profile or cloud security extension

will harmonize these various initiatives. As more cybersecurity communities develop Community Profiles for sectors with different technologies, there is an increasing need for sharing best practices and creating a transparent, consensus-based process with a clear understanding of NIST's role. For example, additional stand-alone guidance could include best practices from developers of existing Community Profiles (e.g., election infrastructure profile, ransomware risk management and communications, cybersecurity manufacturing sectors profiles, etc.).

III. Companion document on utilizing multiple frameworks for organizational risk management

Microsoft acknowledges NIST's commendable efforts to provide important context and connections to NIST resources and relevant frameworks through the development of the NIST Cybersecurity Framework (CSF) Reference Tool and enhancing Cybersecurity and Privacy Reference Tool. We recognize there may be a learning curve and trial-and-error phase to effectively use these dynamic online tools. Once again, we recommend creating a companion document offering guidance for using various relevant frameworks (e.g., CSF 2.0, Software Secure Development Framework (SSDF v1.1), Risk Management Framework (RMF), Artificial Intelligence Framework (AI RMF 1.0), Privacy Framework) for managing organizational risk. The NIST Interagency Report 8170 could serve as a model for creating such a document.

IV. Industry engagement in developing the NIST Cybersecurity Framework (CSF) Reference Tool

Microsoft supports the development of a NIST Cybersecurity Framework (CSF) Reference Tool to host the CSF 2.0 Core which includes both human and machine-readable formats. We also recommend several rounds of industry engagement, feedback, and modification to address complexities and further refine the tool. In the initial stages, NIST could provide education and support, demonstrating how the tool can navigate and discover relationships and dependencies among the datasets and build profiles, overlays, baselines, and templates based on the NIST-referenced data.

V. Fostering robust industry engagement to achieve a continuous feedback loop

We recognize NIST has remained committed to core development principles such as flexibility and interoperability which will ensure the framework's longevity without frequent revisions. However, we feel it is crucial to establish an ongoing feedback mechanism by utilizing existing channels or creating new ones. This is especially important given the introduction of online dynamic tools like CPRT, OLIR, and the CSF reference tool in the context of our ever-changing threat and technological landscape.

VI. Specific detailed revisions to public draft CSF 2.0 Core

a. In Appendix B, under third-party cybersecurity risks, the CSF 2.0 states that "the organization collaborates with suppliers and proactively manages its relationships with suppliers and downstream dependents (e.g., customers). Third parties include more than suppliers (e.g., partners), so we recommend changing suppliers to third parties, or providing more examples of third parties.

b. PR.PT-04 moved to PR. AA-07, however, PR.AA-07 does not exist.

c. DE.DP-02 moved to DE.AE and it is not clear if that subcategory moved to the DE.AE category in a wholesale, generic sense, or to a particular subcategory within that category. Also, consider moving, DE.DP category and subcategory definitions to DE.CM.

d. Add 'periodically reviewed' at the end of ID.AM.08 which currently says 'systems, hardware, software, and services are managed throughout their lifecycle.

e. The current language for PR.AA-01 says identities and credentials for authorized users, services, and hardware are managed by the organization (formerly PR.AC.01). We recommend using the language for PR.AC.1 from CSF v1.1 which states 'identities and credentials are issued, managed, verified, revoked, and audited for authorized devices and users and processes. The inclusion of revoked ensures a cadence for ensuring access is maintained for only individuals that need it.

f. It is unclear who should validate reports in RS.MA-02 which says incident reports are triaged and validated. We recommend including the reports should be validated by internal teams, which align with RS.CO-02 which says internal and external stakeholders are notified of incidents and RS.CO-03 which says information is shared with designated internal and external stakeholders.

Conclusion

Microsoft is grateful for the opportunity to reiterate its commitment to collaborating with industry and government stakeholders over the long term to develop, use, and understand the impact of cybersecurity risk management approaches. We believe that public-private partnerships, international standards, and best practices, like those integrated into the Framework, are indispensable for advancing cybersecurity risk management globally.

Respectfully submitted,

Patricia Ephraim Eke

Director, Customer Security and Trust,

Corporate, External & Legal Affairs

Microsoft Corporation