Microsoft

January 19, 2018

U.S. Department of Commerce
National Institute for Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: Feedback and comments on (Draft 2) Cybersecurity Framework Draft Version 1.1, submitted via email to cyberframework@nist.gov

Dear Mr. Barrett,

Microsoft welcomes the opportunity to provide feedback and comments to the National Institute of Standards and Technology (NIST) on (Draft 2) Cybersecurity Framework Draft Version 1.1 ("Framework v1.1 Draft 2"). As a global technology provider serving more than one billion customers, Microsoft devotes significant resources to improving the security of our products and services and to partnering with others to drive security advancements across the ecosystem. Since 2013, we have contributed our lessons learned from those investments as an active participant in NIST's open, collaborative, and iterative processes for developing and evolving the Framework. We continue to appreciate NIST's approach to not only engaging industry stakeholders but also incorporating stakeholder feedback.

Our perspective on the changes incorporated into Framework v1.1 Draft 2 is derived in part from our experience with using the Framework v1.0. Microsoft has integrated the Framework v1.0 into our enterprise risk management program and regularly uses it to communicate our self-assessment of security capability across senior management and with our Board of Directors. In addition, in support of Federal agencies' required use of the Framework, Microsoft has developed an Azure Blueprint Customer Responsibilities Matrix, identifying areas of the Framework that Azure can implement on an agency customer's behalf.[1] More broadly, we have an ongoing dialogue with partners and customers about use of the Framework as a global cybersecurity risk management best practice relevant across sectors.

Overall, Framework v1.1 Draft 2 is a helpful update that reflects a balance of stakeholder input on v1.1 Draft 1. In particular, the revisions to Section 4.0 help to clarify the potential value and limitations of using measurement information, and the Draft Roadmap outlines a reasonable program to further explore such issues. Specifically, the revised draft captures how the Framework facilitates assessing security capability, setting a Target Profile based on risk and mission/business priorities, and tracking progress in closing gaps. It also captures how the significance of measurement information is undercut without sufficient context or purpose; such information may not only act as an artificial indicator but also undermine the potential of the Framework to drive executive awareness as well as a culture of continuous improvement.

Microsoft offers the following recommendations as NIST moves toward finalizing Framework v1.1 Draft 2 and planning future activities, including those highlighted within the Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1 ("Draft Roadmap"):

- Facilitate use of the Framework for tracking continuous improvement;
- Use NIST's platform to build on the Framework's function as a cross-sector baseline; and
- Continue to drive informed use of the Framework across the ecosystem.

[1] https://blogs.msdn.microsoft.com/azuregov/2017/05/23/azure-blueprint-illustrates-the-clear-path-to-meet-the-cybersecurity-executive-order/

Facilitate use of the Framework for tracking continuous improvement

Framework v1.1 Draft 2 includes substantial updates to the Implementation Tiers, especially within the external participation property. In feedback to NIST during previous comment opportunities, Microsoft has supported clarifications to the Tier criteria[2] as well as a focus on attributes that cut across domain areas.[3] Consistent with that feedback, we applaud NIST for maintaining three properties and better clarifying the differences between adjacent Tiers within Framework v1.1 Draft 2.

Going forward, we encourage NIST to limit substantial updates to the Implementation Tiers and, when substantial updates are warranted, to provide practitioners with an explanation of the intended impacts of Tier criteria changes. Substantial updates necessitate program re-engineering and can disrupt efforts to track progress over time among organizations that have built tools and educated stakeholders based on previous iterations of Tier criteria. Microsoft, for example, has used the Framework v1.0 Tier criteria to develop training and tooling, which we use with practitioners and service owners as well as with executives that track our self-assessment progress and accordingly shift accountabilities and investments. When substantial updates are warranted, an explanation of their intended impact would help ERM professionals re-engineer systems so that new assessments can be measured against previous assessments, supporting programs focused on continuous improvement.

Use NIST's platform to build on the Framework's function as a cross-sector baseline

Consistent with current trends in the cybersecurity ecosystem, Framework v1.1 Draft 2 includes new Categories and/or Subcategories for supply chain risk management, identity management, hardware integrity, and coordinated vulnerability disclosure (CVD); the Draft Roadmap also outlines NIST's plan to take on additional activities or expand the Informative References for some of these areas.[4] As a trusted convener and subject matter expert, NIST is well positioned to help stakeholders better understand how to use "the changing and growing" landscape[5] of cybersecurity standards and recommended practices in a way that's complementary to the Framework. Moreover, NIST seems well aligned with industry in articulating a range of Roadmap topics and pointing to relevant references.[6]

In driving greater awareness of these topic areas and resources, NIST must retain a clear governance role while continuing to cultivate stakeholder engagement. As such, we encourage NIST to differentiate Roadmap work items that are intended to be integrated into the Framework from those that, in the near term, are intended to advance the broader ecosystem. In addition, we are supportive of NIST moving to a more agile process for generating input on standards and other guidance—with the expectation that an online catalogue with a range of relevant material will be distinct from the Framework Core's Informative References.[7] Consistent with NIST's current approach, formally included Informative References should

[2] https://www.nist.gov/sites/default/files/documents/2017/02/14/20160223_microsoft.pdf
[3] https://www.nist.gov/sites/default/files/documents/2017/04/20/2017-04-10_-_microsoft.pdf
[4] In the Draft Roadmap, NIST commits to: promoting the mapping of existing supply chain risk management standards, practices, and guidelines to the Framework Core; partnering with commercial, federal, and international partners to enhance identity management standards/drive adoption of relevant technologies; and raising awareness of CVD among industry.
[5] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf
[6] In responses to Framework v1.1 Draft 1, numerous stakeholders recommended standards and guidelines relevant for inclusion in the Framework, and most of those were also referenced in the Draft Roadmap (i.e., ISO/IEC 27036 and NIST SP 800-161 for supply chain risk management, FIDO protocols for identity management, and ISO/IEC 29147 and ISO/IEC 30111 for CVD were referenced, though NIST SP 800-147 and NIST SP 800-193 for hardware integrity were not).
[7] The Draft Roadmap outlines a plan to transition the Informative References to an online catalog that stakeholders can add to, search, and use and that NIST can govern and draw from as appropriate.

be mature and broadly applicable and have demonstrated value as well as international relevance. Meanwhile, other standards and recommended practices that intersect with, or explore in greater depth, Core topics could be appropriately included in an online catalog or discussed during workshops or trainings. This approach should help NIST balance the need to evolve the Framework to reflect the changing ecosystem with the need to ensure sufficient consistency and ease of use for stakeholders.

We also encourage NIST to prioritize among the many important topic areas and activities outlined in the Draft Roadmap, taking on a mix of deliverables with different time horizons. For instance, from our perspective, CVD and supply chain risk management are among the topic areas that should be prioritized, but CVD is a narrower topic, and existing guidance is more comprehensive and mature. NIST could likely include the two leading international standards as Informative References (within Subcategory RS.AN-5) relatively quickly. Then, NIST could further support ecosystem awareness and understanding by hosting a workshop or webinar, providing both basic CVD guidance for beginners as well information on ISO/IEC 29147 and ISO/IEC 30111 for more advanced stakeholders. Alternatively, supply chain risk management is a complex topic, and while some guidance exists, practices are evolving. The updated Core appropriately includes important steps, such as identifying, assessing, and managing requirements for suppliers and third-party partners; additional standards or guidance for those activities could also be helpful. However, within the Draft Roadmap, NIST should consider narrower topic areas and activities that would address parts of this broad problem space; for instance, NIST could convene stakeholders to capture existing best practices as well as evolving approaches to software assurance. Ultimately, resulting findings could not only support the inclusion of a new supply chain risk management subcategory, articulating baseline guidance for software buyers, but also drive other ecosystem activities.

Continue to drive informed use of the Framework across the ecosystem

The Draft Roadmap not only outlines NIST's next steps in supporting stakeholders' understanding of topic areas such as supply chain risk management but also describes NIST's intention to undertake a range of efforts that will drive uptake and effective implementation of the Framework. To help clarify the intended role of the Roadmap, NIST could more clearly differentiate between substantive updates and activities and other ecosystem support or advocacy efforts (e.g., Roadmap sections 4.2, 4.4, 4.7, and 4.11 verses sections 4.1, 4.3, 4.5, 4.6, 4.8, 4.9, and 4.12). NIST has a significant role to play in both areas, but the stakeholder communities that NIST engages to do so may vary, so helping stakeholders efficiently understand where and how to plug in to different efforts will increase and enhance participation.

We commend NIST for taking on efforts to drive awareness and use of the Framework with a diverse set of communities. As outlined in Section 4.8, NIST has engaged with other governments to support global uptake and within the International Organization for Standardization to demonstrate the Framework's consistency with existing international standards. We encourage NIST to continue these efforts and to partner with other U.S. departments and agencies, including the International Trade Administration, Dept. of Homeland Security, and State Dept., to intensify global advocacy.[8] In addition, as outlined in Section 4.12, we support NIST's efforts to engage small and medium-sized businesses (SMBs) on use of the Framework and complementary tools and guidance. As there are numerous organizations and campaigns focused on SMBs, NIST is well positioned to inform and interface between efforts, amplifying their collective impact. More specifically, we encourage NIST to work with multiple partners to reach different audiences and to share and integrate lessons learned across those partners.

[8] https://www.nist.gov/sites/default/files/documents/2017/04/20/2017-04-10_-_microsoft.pdf

We also encourage NIST to prioritize its investments in supporting the Framework ecosystem, amplifying or augmenting efforts that are most well aligned with the Framework's unique value. In particular, we encourage NIST to use this lens in the context of measurement and confidence mechanisms (i.e., Draft Roadmap sections 4.1 and 4.9). Self-assessments, audits, and other methods of assurance can provide useful feedback to organizations internally as well as sustain trust externally; however, not all methods will have an equally positive impact on Framework use. Recognizing NIST's interest in supporting a diverse market of confidence mechanisms, we also urge NIST to seek or support the development of assurance programs that focus on process—rather than duplicate existing third-party audits that already assess compliance with more prescriptive controls. An assessment program that reflects the Framework's unique value add to the ecosystem would instead take on new assurance challenges, such as validating whether risk management processes are in place, affirming executive engagement, and substantiating that security capability conversations are supported across relevant stakeholders.

In closing, we appreciate the opportunity to provide feedback and comments on the Framework v1.1 Draft 2 as well as the Draft Roadmap. As cited above, NIST's model of stakeholder engagement has resulted in a meaningful dialogue with industry and a well-balanced draft update to the Framework v1.1. Going forward, we are encouraged by the range of activities that NIST has outlined in the Draft Roadmap, and we look forward to continuing to partner with NIST to build on the Framework's function as a cross-sector baseline and to drive greater awareness and informed use of the Framework. We also welcome the opportunity to continue our ongoing dialogue with NIST and other stakeholders about the Framework and related efforts to advance security across the ecosystem.

Sincerely,

Angela McKay
Senior Director, Global Security Strategy and Diplomacy
Digital Trust
Microsoft Corporation

Appendix A: Responses to NIST Questions

Question	Microsoft response
Do the revisions in Version 1.1 Draft 2 reflect the changes in the current cybersecurity ecosystem (threats, vulnerabilities, risks, practices, technological approaches), including those developments in the Roadmap items?	Yes – see attached cover letter for details
For those using Version 1.0, would the proposed changes affect their current use of the Framework? If so, how?	Yes – see attached cover letter for details, especially "Facilitate use of the Framework for tracking continuous improvement"
For those not currently using Version 1.0, would the proposed changes affect their decision about using the Framework? If so, how?	n/a