Before the

United States Department of Commerce

and the

National Institute of Standards and Technology

In the Matter of	)	
Views on the Framework for	)	
Improving Critical Infrastructure Cybersecurity	)	RFI Docket # 151103999-5999-01

Response of

Microsoft Corporation

to Request for Information

Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
(425) 882-8080

February 23, 2016

I. INTRODUCTION

Microsoft welcomes the opportunity to provide to the National Institute of Standards and Technology (NIST) comments that reflect our experience with using and our perspective on the future of the Cybersecurity Framework (the Framework). As a provider of technology products and services to more than one billion customers in the United States and around the world, Microsoft is constantly innovating and investing to develop, implement, refine, share, and promote cybersecurity best practices.[1] We also partnered with NIST and various government and industry colleagues to develop the Framework, and we continue to support the Framework's implementation as a basis for harmonizing cybersecurity best practices internationally.[2]

NIST and U.S. government efforts to promote domestic and international use of the Framework have impacted and will continue to significantly impact its adoption and relevance, both within the United States and beyond. In addition, how and by whom the Framework is governed will continue to significantly impact its trajectory, including its potential to harmonize global cybersecurity risk management best practices. We appreciate the opportunity to continue to engage in an open comment process and a robust public-private partnership with NIST as it considers not only how to update and promote broader use of the Framework but also whether to transition governance functions to another organization.

The structure of our Comments is as follows:

- Using the Framework for communication within and between organizations;
- Updating the Framework to foster greater usability;
- Promoting domestic and international use of the Framework; and
- Defining an approach for long-term governance of the Framework.

Enclosed in Appendix A are our specific responses to NIST's 25 Request for Information (RFI) questions.

II. USING THE FRAMEWORK FOR COMMUNICATION WITHIN AND BETWEEN ORGANIZATIONS

Microsoft is using the Framework to supplement internal communication about our cybersecurity risk management maturity. As part of our enterprise risk management program (ERM), we have assessed how our cybersecurity risk management practices align with those included within the Framework's guidance. We first assessed our largest cloud services,[3] and we are now expanding our assessment to additional services. As our risk management teams developed an assessment methodology, they valued the Informative References' direct mapping

[1] *See, e.g.*, https://training.safecode.org/resourcecenter; https://blogs.microsoft.com/cybertrust/2015/10/07/whats-new-with-microsoft-threat-modeling-tool-2016/. Through SAFECode, Microsoft shares information about our Security Development Lifecycle (SDL), a security assurance process that reduces the risk of product vulnerabilities and protects against their malicious or inadvertent introduction by requiring rigorous security engineering and software review processes. http://www.microsoft.com/security/sdl/default.aspx.

[2] http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf (at 1-3).

[3] http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf (at 3).

to ISO/IEC 27001 and NIST SP 800-53, which accelerated their communication with other internal teams by establishing an immediate link with other ERM and certification efforts.[4]

Microsoft also envisions using the Framework to enhance internal communication about cyber risks and opportunities and business investments in security. The Framework's Core and Profile portions provide helpful structures for discussing and mapping paths to advancing cybersecurity risk management processes.[5] At a high level, the Functions constitute a clear and comprehensive risk management strategy, helping to structure communication of cyber risks and opportunities across executive levels. The Profile portion also facilitates conversations between and among technical, risk management, and executive leadership teams, acting as an external reference point by which companies can express their current and target states of maturity.

The Framework is also increasingly being used or considered as a mechanism for suppliers to share risk management information. For example, Microsoft's multi-tenant cloud service offerings for Azure, Office 365, and Dynamics CRM Online have achieved multiple global certifications and U.S. authorizations,[6] but conversations in key regulated sectors about our self-assessment against the Framework have provided additional value. In addition, as we build out our existing supply chain risk management programs,[7] Microsoft is exploring how to use the Framework as a mechanism to articulate risk management information.

III. UPDATING THE FRAMEWORK TO FOSTER GREATER USABILITY

The Framework's Profile, Implementation Tiers, and Core can be updated to foster greater usability both within and between organizations. First, the Profile portion can foster greater usability within organizations by preparing risk management teams to lead more nuanced cross-group conversations about varying internal risk postures and business objectives. As the Framework acknowledges, complex organizations may struggle to develop a single, company-wide profile; instead, they may need to develop multiple profiles for different services or business groups. Including guidance around how or why organizations might examine, establish, use, or reconcile multiple Current or Target Profiles would increase the Framework's usability.

Second, greater clarity around the distinctions between adjacent Implementation Tiers would foster greater usability of the Framework within organizations. In their current form, the Tiers are challenging to use because much of the text that differentiates between them creates overlapping metrics, necessitating subjective judgments.[8] As a comparative benchmark, the text

[4] http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf (at 4).
[5] http://csrc.nist.gov/cyberframework/rfi_comments/040713_microsoft.pdf (at 5-7).
[6] http://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27001; https://www.fedramp.gov/marketplace/compliant-systems/.
[7] http://download.microsoft.com/download/9/B/D/9BD9FBFF-A1D9-4DA9-954C-EAE9242C689D/Toward%20a%20Trusted%20Supply%20Chain%20white%20paper.pdf.
[8] For example, for Tier 2 Risk Management Processes, risk management practices are "*approved* by management but *may not* be established as organizational-wide policy," and "prioritization of cybersecurity activities is directly informed by organizational risk objectives, the *threat environment*, or *business/mission objectives* (emphasis

that differentiates between Tiers with regard to external participation creates more distinct metrics. Moreover, given that organizational goals, business needs, and risk management practices more aptly fit along sliding scales than in artificial groupings, the Framework could more usefully describe attributes that could then populate Current and Target Profiles.

Third, guidance that emphasizes and further develops the Core's focus on security outcomes will foster greater usability of the Framework between organizations. In particular, among organizations that are assessing whether service providers meet their security needs, additional NIST guidance could help to instill the norms of 1) having risk-focused conversations with providers from the outset and 2) accepting alternative security measures. Organizations that absorb these norms will evolve their enterprise infrastructure strategies, enabling assessment and, as appropriate, adoption of new technologies and services, including cloud computing.

Guidance that clarifies the intent and context behind the Framework's Categories and Subcategories could help organizations focus on security outcomes rather than on controls implementations. Controls provide a valuable way to consistently measure security practices, but in our experience, organizations that focus *exclusively* on controls miss an opportunity for more informative risk management conversations. Instead, as organizations evaluate whether service providers meet their security needs, they should: 1) clearly articulate their security outcomes; 2) determine specific use cases for priority risk events; and 3) accept multiple ways to meet or exceed those outcomes, including alternative security measures.

For example, as the Framework articulates, the intended security outcome of the Access Control Category is to allow only authorized users or devices with access to particular assets. Both a stipulated set of controls, including one pulled from the Informative References, and particular technology capabilities or features, such as multi-factor authentication, may support that outcome, either independently or jointly. As such, rather than focusing solely on a control implementation, organizations should be open to conversations with providers about technology capabilities or features that address their risk priorities and scenarios. Through this broader evaluation, which additional NIST guidance could drive, both security outcomes and business objectives, such as increasing organizational agility through new technology, can be considered.

The Framework could position organizations to discuss security outcomes with their providers from the outset by including guidance that emphasizes and further develops the Core's method of taking a risk-based approach. In particular, Microsoft's experience working with the U.S. government on integrating cloud services with Trusted Internet Connections (TIC) obligations provides an example of what additional Framework guidance could ultimately support. We have been one of a select group of cloud service providers to pilot our technology with U.S. government agencies as they have tested the FedRAMP TIC Overlay requirements. At the outset

---

added)." For Tier 3 Risk Management Processes, risk management practices "are *formally approved* and expressed as policy," and "organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in *business/mission requirements* and a changing *threat* and technology *landscape*." Neither part of the definitions is sufficiently distinctive to provide a robust measure of maturity.

of the pilot, discussions were focused largely on cross-walking controls intended for the traditional, on-premises environment to cloud services. However, as the discussion re-oriented around desired security outcomes for TIC, rather than solely focusing on compliance against security controls, there were meaningful and outcome-focused discussions around enabling agencies and the Department of Homeland Security (DHS) with the capabilities needed to have insight into who is authenticating, accessing, and exfiltrating .gov data. Only after successful discussions around security outcomes and risk scenarios could we explore alternative, security-equivalent capabilities that are available to agencies to meet the TIC Overlay requirements and DHS's desired outcome of operational visibility. Government and other organizations could use Framework guidance to have security outcome-focused conversations from the outset.

Updating the Framework to foster greater usability both within and between organizations in the three ways described above should be prioritized; then, substantive updates to the Framework are an important next step. Authentication is the most pressing among the substantive areas described within NIST's Roadmap. Numerous U.S. government initiatives, including the National Strategy for Trusted Identities in Cyberspace (NSTIC) and Homeland Security Presidential Directive 12 (HSPD-12), have not resulted in sufficient progress. By developing and mapping Framework guidance to Special Publications that support improved authentication practices, NIST could add valuable momentum to help address a major gap in U.S. government security. NIST could also help the U.S. government to leverage emerging technologies with broad industry support, such as those being developed through the Fast IDentity Online (FIDO) Alliance.

In addition to updates made directly to the Framework, NIST could also foster greater usability by encouraging and partnering with U.S. departments and agencies and other governments to develop sector-specific, control-level references. As part of our effort to self-assess our conformance with the Framework, Microsoft pulled language from the Informative References materials. However, many organizations that would benefit from using the Framework may not have sufficient cybersecurity resources to support that implementation step. In addition, many of the Subcategories point to multiple areas within an Informative Reference, and sector-specific guidance could clarify which control language is most relevant, enabling organizations to implement the Framework more quickly and in a more precise way.

IV. PROMOTING DOMESTIC AND INTERNATIONAL USE OF THE FRAMEWORK

The U.S. government urgently needs a multi-pronged approach for advancing the Framework. Standardization, procurement, capacity building, and information sharing are essential components of such an approach. In addition, the updates described in the previous section will foster greater usability globally. However, in its existing form, the Framework already acts as a valuable reference point for communication within and between organizations and for cybersecurity risk management self-assessments. More strategic promotion of the Framework both domestically and internationally should begin immediately and then continue to build as greater usability is fostered.

Microsoft strongly encourages NIST to promote the Framework as an international standard by working with the private sector to transfer the Framework to an international standards group. Today, more than 80 countries are in the process of creating new cybersecurity regulations, and a myriad of implementing requirements are being considered. Making the Framework an international standard would not only help to improve but also help to harmonize cybersecurity practices on a global scale. U.S. companies will increasingly benefit from using the Framework as it becomes a baseline that influences global discussions around cybersecurity risk management best practices, and such harmonization would also prevent U.S. companies from the disadvantage of needing to comply with multiple or competing domestic approaches. In addition, the Framework is the product of significant industry engagement and best practice sharing, and because its utility has already been validated, encouraging global adoption could significantly advance global ecosystem security.

Utilizing procurement to drive adoption is also a vital step, but NIST advocacy alone is not sufficient. NIST should reference the Framework in its Special Publications, positioning the Framework as a recommended requirement for U.S. government procurement. In addition, the Office of Management and Budget (OMB) should determine how best to align the Framework to Federal Information Security Management Act (FISMA) requirements and ensure that Framework best practices are included in procurement requirements. This OMB step may also require amending the relevant Federal Acquisition Regulations as appropriate.

Moreover, the entire U.S. government must engage much more deliberately in driving global conversations about and raising the visibility of the Framework. The U.S. Department of State should include training on the use of the Framework in all of its global cybersecurity capacity-building efforts.[9] Likewise, the White House should highlight the Framework in its strategic cybersecurity partnerships.[10] As a globally respected government and industry partner, NIST should also continue to facilitate a range of conversations to support implementation of the Framework in the United States and beyond.

I. DEFINING AN APPROACH FOR LONG-TERM GOVERNANCE OF THE FRAMEWORK

NIST should work with the private sector to establish a process for transferring the Framework to an international organization for long-term governance and development. The Framework must move into an appropriate international organization to achieve far-reaching global adoption. In addition, the transition of the Framework's to an international organization must maintain the flexibility, scalability, and inclusivity that have been the hallmarks of NIST's approach.

Depending on their size, sector, maturity, or other factors, organizations may seek to use the Framework differently, including to manage risk, evaluate service providers, and self-assess conformance with best practices. In addition, the Framework is taking root among key enablers

[9] http://www.state.gov/s/cyberissues/releasesandremarks/.

[10] https://www.whitehouse.gov/the-press-office/2015/04/28/fact-sheet-us-japan-cooperation-more-prosperous-and-stable-world; https://www.whitehouse.gov/the-press-office/2016/01/19/fact-sheet-united-states-%E2%80%93-australia-cooperation-deepening-our-strategic.

of adoption, including auditors,[11] insurers,[12] and the legal system.[13] This wide range of ecosystem activities is a positive sign of the Framework's utility and may even expand as greater usability and global adoption are fostered and supported.

A future Framework governance organization must continue to support diverse use, greater usability, and global adoption, so NIST and its stakeholder community should further dialogue as they discern a governance partner that can meet such a challenge. Because NIST is legally authorized by the Cybersecurity Enhancement Act of 2014 to develop best practices such as the Framework,[14] it is within NIST's mandate to continue to govern the Framework until a new governance organization can be identified. As such, NIST should build from the input provided through this RFI to structure opportunities for further discussion. In particular, NIST should convene workshops in the United States and overseas. Input from both U.S. and international organizations and governments will be essential to discerning the appropriate governance organization that will be capable of advancing the Framework globally.

NIST should focus on the attributes that are vital to a future governance organization and the Framework's continued success as it evaluates next steps. Microsoft supports the transitioning of the Framework's governance to an international organization with the following 6 attributes:

1) international mandate and global recognition and respect as a subject matter expert;
2) ability to support various implementation approaches/activities across the ecosystem;
3) expertise across multiple sectors;
4) demonstrated objectivity;
5) unwavering commitment to engaging with a broad stakeholder community, including the private sector; and
6) dedicated, professional staff with technical risk management capabilities.

The above-listed attributes should guide NIST's and the stakeholder community's evaluation of potential Framework governance organizations because those attributes have been vital to NIST's successful governance of the Framework. NIST's expertise across sectors, objectivity, commitment to engaging with a broad stakeholder community, and dedicated staff enabled it to develop valuable cross-sector cybersecurity risk management guidance, and such attributes will also be vital to updating the Framework for greater usability and to broadening its substance. In addition, an international mandate and the ability to support various implementation approaches and activities will foster greater usability and global adoption.

NIST should also focus on an approach and timeline for its governance transition. Microsoft supports an approach in which an organization with the above attributes works with governments around the world to further develop the Framework and refine it for international standardization. Ultimately, much of the governance of the Framework should transition from

[11] https://www.tenable.com/sc-dashboards/cybersecurity-framework-audit-dashboards.
[12] https://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/cybersecurity-exams-insurance.pdf.
[13] http://www.mdchhs.com/wp-content/uploads/UM-CHHS_article_USCYSU14.pdf.
[14] https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

NIST to an international standards organization, though NIST should also continue to maintain a role in guiding U.S. organizations as they implement the Framework. Over the long term, an organization such as the International Standardization Organization (ISO) is well positioned to manage portions of the Framework. However, because of the urgency of advancing the Framework globally and the lengthy process of developing an international standard, moving the Framework to an interim international organization with the above-described attributes is an important and pressing first step. Microsoft supports a timeline in which NIST immediately begins to convene international stakeholders to evaluate potential interim governance organizations. Taking this step immediately will not only help NIST to build on the momentum of this RFI but also elevate the visibility of the Framework, helping countries that are developing cybersecurity policies and regulations to understand the approach used to build the Framework, its risk management focus, and its global relevance.[15] Within 12 months, NIST should formulate a plan for transitioning the Framework and begin the international standard development process.

II. CONCLUSION

The Framework has established a meaningful way for Microsoft to discuss, assess, and refine our cybersecurity risk management maturity. Updates to the Profile, Implementation Tiers, and Core will foster greater usability, and substantive updates, especially to support additional NIST guidance around authentication, will add important value. Going forward, governance of the Framework will significantly impact its adoption, use, and influence across sectors, markets, and borders. To manage a transition to an appropriate governance organization, NIST should convene workshops in the United States and overseas to discuss the attributes that are vital to a future governance organization and to the Framework's continued success.

We thank you for the opportunity to contribute to the Framework development process and to engage with NIST as an industry partner. We would also welcome the opportunity to continue with NIST the conversation that this RFI has initiated.

Sincerely,

J. Paul Nicholas
Senior Director, Global Security Strategy and Diplomacy
Trustworthy Computing, Microsoft Corporation

Appendix A: Microsoft_december-2015-response-template_20151211

[15] During these conversations, NIST could also highlight how the Framework has been successfully adapted globally, such as by the Italian government. http://www.cybersecurityframework.it/.

Organizational Information
Organization Name
Organization Sector
Organization Size
Organization Website
Organization Background
Point of Contact Information
POC Name
POC E-mail
POC Phone

Response
Microsoft
Information Technology
around 112,000 employees worldwide
microsoft.com/cybersecurity

Microsoft is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more.

Response
Amanda Craig
amcraig@microsoft.com

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Microsoft is a leading provider of technology products and services to more than a billion customers in the United States and abroad. Microsoft has been deeply engaged in the Framework development process because we view the Framework as an important reference point for domestic and international efforts to improve critical infrastructure cybersecurity.	http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	We are responding as a user and subject matter expert.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Microsoft is using the Framework to supplement our risk management program and as a communication tool. We are also evaluating potential use of the Framework as a supplier and vendor management tool.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	We have leveraged all portions of the Framework.	
5	What portions of the Framework are most useful?	The Framework Core and Profile portions for the reasons described in the attached letter.	
6	What portions of the Framework are least useful?	The Implementation Tiers portion for the reasons described in the attached letter.	
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	Greater usability of the Framework could be fostered by updating the Core, Profile, and Implementation Tiers as described in the attached letter.	
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	As a leading global technology provider, Microsoft already had in place before the release of the Framework a robust risk management program, so the Framework has not helped to reduce our cybersecurity risk. However, the Framework has been very useful in helping us to understand the relative value of investments and to track our maturity.	
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	In addition to considering these questions in the domestic context, we encourage NIST to consider these questions in the global context.	
10	Should the Framework be updated? Why or why not?	Yes, to address the opportunities to foster greater usability described in the attached letter.	
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.	The Profile, Implementation Tiers, and Core should be updated to foster greater usability as discussed in the attached letter.	
12	Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?	Standards that the Framework references should be updated on an ongoing basis. As the industry continues to evolve, new standards that may be relevant to supporting the Framework should also be evaluated and added on a regular basis.	
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?		

#	Question Text	Response Text	References
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	Yes. Among the areas identified in the Roadmap, authentication is the most important and pressing to address.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Updating on an ongoing basis the Framework's Informative References will not impact use. With a publicly shared update cadence, stakeholders can also accommodate cycles of updates to other portions of the Framework.	
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?	One-on-one engagements with NIST and with peer stakeholders have been most useful for informing our use of the Framework.	
17	What, if anything, is inhibiting the sharing of best practices?		
18	What steps could the U.S. government take to increase sharing of best practices?	As discussed in the attached letter, the U.S. government should engage much more deliberately in driving global awareness and use of the Framework. For instance, the U.S. Department of State should reference the Framework in all of its global cybersecurity capacity-building efforts.	
19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?	An ongoing program in which NIST convenes and facilitates conversations to support implementation, including amongst public and private stakeholders of various sizes and within various market sectors around the world, would create a forum in which organizations can regularly share information about their experiences.	
20	What should be the private sector's involvement in the future governance of the Framework?	As discussed in the attached letter, NIST should focus on the desired attributes of a future governance organization.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Yes, in the way described within and according to the criteria outlined in the attached letter.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	As the Framework is transitioned to an organization the meets the criteria described in the attached letter, this question should be revisited.	
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	NIST should first focus on the attributes rather than the address or type of future Framework governance organization.	
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?	Once an organization is identified, a transition plan can address steps to minimize or prevent disruption.	
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?	A future Framework governance organization should have the following attributes: 1) international mandate and global recognition and respect as a subject matter expert; 2) ability to support various implementation approaches and activities across the ecosystem; 3) expertise across multiple sectors; 4) demonstrated objectivity; 5) unwavering commitment to engaging a broad stakeholder community, including the private sector; and 6) dedicated, professional staff with technical risk management capabilities.	