Before the

United States Department of Commerce

and the

National Institute of Standards and Technology

In the Matter of	)	
Experience with the Framework for	)	
Improving Critical Infrastructure Cybersecurity	)	RFI Docket # 140721609-4609-01

Response of

Microsoft Corporation

to Request for Information

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

October 10, 2014

I. Introduction

Microsoft welcomes the opportunity to comment on our experience with the National Institute for Standards and Technology (NIST) Cybersecurity Framework (the Framework). As one of the leading providers of technology products and services to billions of customers in the United States and abroad, we hope that our comments will help inform the U.S. Government's ongoing efforts to advance cybersecurity through the Framework and other initiatives.

Microsoft provided significant contributions to the Framework development process because we view the Framework as an important reference point for domestic and international efforts to improve critical infrastructure cybersecurity. Both in terms of how the Framework was developed and its substantive guidance, the Framework sets a high mark for public-private and cross-sector collaboration. We were also highly supportive of the voluntary approach to the Framework set forth in Executive Order 13636 (the EO). We have continued our support for EO initiatives through participation in both international and domestic engagements to raise awareness of the Framework. Additionally, we have made similar investments in assessing our policies and practices against the Framework.

Looking forward, however, we are concerned that the Framework's utility will be undermined by uneven progress in the implementation of the EO as well as disharmony in the U.S. Government's use of various standards and requirements to enhance cybersecurity across Government and critical infrastructures.

Specifically, Microsoft encourages the U.S. Government to invest in full execution of the EO, particularly the Framework-support incentives prescribed there. We also encourage NIST to harmonize the Framework and its Roadmap across the U.S. Government's growing body of relevant work, such as FedRAMP and supply chain standards. Finally, we encourage NIST to refine its future Framework outreach activities to address the Framework's relevance to technological advancements that are common across sectors, like cloud computing.

Microsoft applauds NIST for its dedication in developing and improving the Framework. We look forward to continued dialogue with NIST -- and others in government and industry -- to advance cybersecurity.

II. Microsoft's Investment in the Framework Development Process and Raising Framework Awareness

Microsoft's high level of familiarity with the Framework is an outgrowth of our contributions to the Framework development process.[1] Specifically, we provided comments in response to NIST's initial request for information[2] and NIST's request for comments on Preliminary Framework.[3] We also participated in regional workshops hosted by NIST[4], and we hosted an

[1] This paragraph responds to questions 2 and 8 of the *Current Awareness* section of the RFI.
[2] http://csrc.nist.gov/cyberframework/rfi_comments/040713_microsoft.pdf
[3] http://csrc.nist.gov/cyberframework/framework_comments/20131213_jpaul_nicholas_microsoft_part1.pdf
[4] http://www.nist.gov/itl/csd/cybersecurity-framework-webcast.cfm

event[5] at our Policy and Innovation Center in Washington, DC that brought together security and privacy professionals, helping to engage the privacy community[6] alongside representatives from critical sectors.

Subsequent to the Framework's release, Microsoft has helped to raise awareness and understanding of the Framework outside of the United States while also engaging domestically.[7] For example, Microsoft played a leadership role in a public-private delegation to Korea and Japan to share perspectives on national cybersecurity efforts, including the Framework. Similarly, we conducted a series of cybersecurity workshops in Europe and South Africa that focused on critical infrastructure protection and the functions-based approach put forward in the Framework. In specific settings, we have raised awareness of the Framework with international organizations in Africa and the Middle East. We have also engaged in domestic outreach on the Framework, including participation in the U.S. Chamber of Commerce's targeted campaign to engage critical infrastructure owners and operators around the country.[8]

Microsoft invested in the Framework development process and awareness activities because we expect that both public and private sector customers, including critical infrastructures, will continue to seek greater understanding of their vendors' cybersecurity practices. Like other companies that serve customers in the United States and overseas, we want cybersecurity risk management requirements to be outcome-focused, standards-based, and harmonized to the greatest degree possible both domestically and internationally.

With respect to NIST's inquiries about international awareness of the Framework, Microsoft is concerned that international awareness remains fairly low.[9] While some government and industry leaders outside of the United States may have heard about the Framework, we are unaware of any concerted effort by the U.S. Government to help foreign governments or private sector organizations understand the Framework and contemplate its utility. U.S. industry has attempted to fill the void, and we encourage the U.S. Government to articulate its plan to raise international awareness and understanding of the Framework.

Moreover, the uneven implementation of Framework-support mechanisms set forth in the EO, such as incentives, has the potential to compromise the U.S. Government's global leadership on cybersecurity policy. Prior initiatives like the Comprehensive National Cybersecurity Initiative had global impact because they set a new high bar for cybersecurity investment by a national government. Today, the steady progress of the European Network and Information Security Directive (NIS Directive) has heightened international awareness and interest in the EO's voluntary strategy. Various drafts of the NIS Directive have proposed more regulatory approach than the EO, and countries in Europe and beyond are monitoring policy outcomes in the U.S. and Europe. It is an open question whether the EO's voluntary approach will prove persuasive

[5] http://blogs.microsoft.com/cybertrust/2013/10/31/microsoft-hosts-cybersecurity-and-privacy-professionals-for-discussion-about-the-cybersecurity-framework/
[6] https://privacyassociation.org/news/a/privacy-professionals-needed-in-nist-framework-process/
[7] This paragraph responds to questions 6 and 8 of the *Current Awareness* section of the RFI.
[8] https://www.uschamber.com/event/strengthening-cyber-supply-chain-against-malicious-hackers-exploration-new-cybersecurity
[9] This paragraph responds to questions 8 and 9 of the *Current Awareness* section of the RFI.

without activities that catalyze use of the Framework. Accordingly, it is important for the U.S. Government to recognize that there are significantly different models under consideration in Europe and the United States, and U.S. leadership will depend on the Government's ability to fully execute the EO.

Domestically, it seems that interest in the Framework is strong, but understanding of the Framework's voluntary nature, structure, and overall purpose has really taken root only amongst organizations that invested in the Framework development process on some level.[10] Setting aside those companies that participated in the Framework development process, there does not seem to be a critical mass of companies ready to leverage the Framework as a "go to" cybersecurity baseline. Now that there are several campaigns underway to increase awareness of the Framework, it is likely that overall understanding of the Framework will increase, but whether critical infrastructure organizations utilize the Framework at scale will likely depend on implementation of the EO mechanisms intended to encourage Framework use.

III. Microsoft's Alignment with the Framework

Microsoft has leveraged the Framework as part of our enterprise risk management program. In addition to utilizing the Framework at the enterprise level, our largest cloud services conducted service-level assessments against the Framework to examine their alignment.[11] Because Microsoft has a robust focus on cybersecurity and privacy in our enterprise and service-level risk management programs, and because the Informative References in the Framework draw from well-known IT security standards, the Framework's security guidance was fairly easy to digest by our security risk management professionals.

Based on our cross-company self-assessment, Microsoft determined that our security policies and practices are consistent with the Framework. Our alignment with the Framework rests upon Microsoft's security strategy, which is rooted in policy, standards, and procedures that are tested and validated through a cross-company process. To help demonstrate our commitment to security, we invest in third-party certifications against certain international and national standards and requirements to meet our customers' expectations. Specifically, there are two ways in which our certification activities relate to the Framework:

- third-party certifications of our cloud services against ISO/IEC 27001 and NIST SP 800-53; and
- third-party certifications of our cloud services under FedRAMP, the U.S. Government's threshold security requirements for cloud service providers (CSPs) who wish to sell to U.S. Government agencies.

First, several of Microsoft's cloud services – Azure, Dynamics CRM, Global Foundation Services, Office 365, and Yammer – are currently certified against ISO/IEC 27001:2005. In addition to this certification, three services – Azure, Global Foundation Services, and Office 365 – are certified against FISMA, which is based upon the NIST SP 800-53 controls. These

[10] This paragraph responds to question 1 of the *Current Awareness* section of the RFI.
[11] This paragraph responds to question 1, 2, 6, and 8.a. of the *Experiences* section of the RFI.

certifications are highly relevant to any discussion of the Framework Core because nearly all of guidance provided in the Framework is drawn from these standards.

Next, both Azure and Global Foundation Services are certified under FedRAMP. Although FedRAMP is not included as an Informative Reference in the Framework, FedRAMP certifications are demonstrative of Microsoft's commitment to meeting the U.S. Government's requirements for cloud service providers. Cloud services that meet the U.S. Government's own security standards support a large number of the security outcomes put forward in the Framework Core, particularly because FedRAMP is essentially a cloud-adapted version of NIST SP 800-53.

With respect to NIST's interest in which elements of the Framework were most helpful, Microsoft found the Framework's direct mapping to ISO/IEC 27001 and NIST SP 800-53 to be particularly helpful.[12] First, the mapping established an immediate linkage between our ongoing risk management and certification efforts. The mapping also continues to provide an extremely helpful example to share with governments outside of the United States that may be considering a national cybersecurity framework. By mapping the Framework's security guidance to an international standard, NIST has demonstrated that national cybersecurity concerns can be addressed in alignment with standards. In fact, Microsoft would encourage NIST to continue this exercise and include FedRAMP mapping as in scope as well, in order to help government agencies and others understand the security framework for cloud use and adoption in the U.S.

In contrast, from our perspective as a large, complex, and globally-distributed organization, Microsoft found the Framework Implementation Tiers to be unhelpful.[13] For organizations that have invested heavily in risk management policies and programs, parsing the difference between the Tiers provides limited value. Unless an organization is considering gaps that span more than one Tier, the difference between adjacent Tiers seem minimal. Moreover, because the Tiers are subjective, they are particularly prone to differing interpretations. In our experience with the Tiers, it was easy for risk management professionals to identify the same activity set at two different adjacent Tiers. Moving forward, tightening up the definitions so that they are more distinct would be helpful in a future version of the Framework.

Finally, with respect to NIST's interest in how organizations have leveraged the Framework to discuss cybersecurity risk management, Microsoft has used the Framework in some C-suite communications and discussions with customers.[14]

IV. The Future of the Framework and Executive Order Implementation

Microsoft has consistently praised the Framework because it was developed using an open and inclusive process, and the resulting approach is risk-based and maps directly with international standards. However, we are concerned that the Framework faces an uncertain future without

[12] This paragraph responds to question 4 of the *Experiences* section of the RFI.
[13] This paragraph responds to question 4 of the *Experiences* section of the RFI.
[14] This paragraph responds to question 8.d. of the *Experiences* section of the RFI.

implementation of the Framework support mechanisms set out in the EO, primarily incentives for organizations that utilize the Framework.

The Framework may provide a substantive baseline for organizations that are developing or assessing a cybersecurity risk management program, but there is not necessarily a business case for an organization to use the Framework. Microsoft will continue to invest in cybersecurity risk management because it clearly aligns with our customers' interests; other organizations may not feel compelled to do the same without government incentives. From a public policy perspective, if the Administration wants to see improvement in the national cybersecurity baseline, then policies will need to catalyze action by broader swaths of the computing ecosystem where market dynamics alone will not drive investment in cybersecurity risk management.

The lack of meaningful progress on incentives for organizations that use the Framework stands in sharp contrast to the deep investment by stakeholders in the Framework development process.[15] For nearly 12 months, hundreds of organizations participated in NIST's public comment opportunities, workshops, and a breadth of associated events within their respective sectors. Following the Framework's release, the stakeholder community has little more than an a few agency reports and a blog post from the White House about potential incentives for Framework use. During the same period, there have been several comments from U.S. Government officials indicating that organizations must invest more deeply in advancing the Framework or regulation may be necessary. These comments seem at odds with the structure put forward in the EO, which is clear that voluntary use of the Framework was intended to be driven by incentives.

Moreover, these statements reflect a need for greater understanding about the private sector, particularly business processes, industry procurement and capital investment cycles, and the complexities of corporate IT systems and deployments. In many cases -- particularly for large, multi-national corporations – it is highly resource-intensive to conduct a comprehensive assessment of the various global compliance implications of adapting security policies and approaches. These processes can be expedited when a requirement set emerges that is supported by tangible market demand but, without incentives, the Framework lacks such demand at this time.

In response to NIST's inquiry concerning the role of the Department of Commerce's Internet Policy Task Force (IPTF) and Commerce agencies in promoting the Framework, it would be helpful to see a reinvigorated IPTF play a more meaningful role in advancing the private sector's perspective in overall cybersecurity policy development.[16] Following the release of Commerce's Green Paper on Cybersecurity, Innovation, and the Internet Economy, it seems that the IPTF's cybersecurity work has been fairly limited.[17] During the same period, the sheer volume of policy issues and technological developments with significant ramifications for U.S. IT companies has increased sharply.

[15] This paragraph responds to question 2 of the *Roadmap* section of the RFI.
[16] This paragraph responds to question 9 of the *Experiences* section of the RFI.
[17] http://www.ntia.doc.gov/category/cybersecurity

One area where the IPTF could help advance the Framework and cybersecurity overall is to convene cross-sector dialogues about the Framework's applicability in different IT environments. For example, critical infrastructure organizations are increasingly reliant on cloud services. The IPTF could bring together security practitioners from critical sectors that are using cloud services, alongside cloud service providers (CSPs), to share perspectives on the Framework's applicability to cloud deployments. The benefit of this dialogue would be better understanding across sectors of how cloud usage can improve cybersecurity risk management in many instances, and assist critical infrastructure organizations in aligning with the Framework. Given that cloud computing touches upon the organizational equities of multiple Commerce Department agencies, the IPTF is well-positioned to convene this dialogue.

With respect to NIST's interest in whether its Roadmap is focused on the right areas for further development, Microsoft feels that the Roadmap's substantive focal points are correct.[18] However, there are a number of key questions that NIST should answer before seeking additional investment from stakeholders in the Framework. For example, NIST has identified supply chain risk management as an area for further development. There are both national (draft NIST SP 800-161) and international standards (draft ISO/IEC 27036) that are under development in this area, and organizations like Microsoft are already contributing to these processes. It is unclear what another NIST work stream on supply chain risk management would add and how it would interface with the international process.

Finally, because many organizations are not yet familiar with the Framework, moving towards an updated version seems premature at this time. While we encourage NIST to map FedRAMP to the Framework, we think that NIST should refrain from initiating work towards a second iteration of the Framework until at least one year has passed since its publication to allow for greater awareness and understanding of the Framework in critical sectors. Moreover, as discussed above, it will continue to be important for NIST to demonstrate how work towards a second version of the Framework is integrated with other standards and procurement work underway in the U.S. Government, as well as international cybersecurity initiatives.

V. Conclusion

In conclusion, Microsoft appreciates the opportunity to comment on our experience with the Cybersecurity Framework. We look forward to continued dialogue with NIST -- and others in government and industry -- to advance cybersecurity.

[18] This paragraph responds to question 1 of the *Roadmap* section of the RFI.