Before the
United States Department of Commerce
National Institute of Standards and Technology

In the Matter of	)	
	)	
Request for Comments	)	Docket No. 130909789-3789-01
On the Preliminary Cybersecurity	)	
Framework	)	
	)	

Response of Microsoft Corporation to Preliminary Cybersecurity Framework

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

December 13, 2013

I. EXECUTIVE SUMMARY

Microsoft commends the National Institute of Standards and Technology (NIST) on its continued work on the Preliminary Cybersecurity Framework,[1] which represents a significant step towards broadly-applicable cybersecurity guidance for critical infrastructure organizations and others that seek to improve their cybersecurity policies, practices, and procedures.[2] The Framework's structure and content, particularly its reliance on international standards and well-known cybersecurity guidelines, present a baseline for organizations to develop and assess cybersecurity risk management as needed for their business objectives.

To maximize the potential positive benefits of the Framework for implementing organizations and others, Microsoft suggests four actions that NIST should take in the final development of the Framework: expand the Framework's security guidance related to secure engineering and asset management; focus the Framework's privacy guidance; streamline the Framework's structure; and allow an additional opportunity for public comment on the Framework prior to its final release in February.

These areas and related recommendations are visually represented as follows, and described in greater detail below:

Areas for Further Action	Recommendations	Rationale
Expand the Framework's security guidance related to secure engineering and asset management	• Broaden the discussion of secure engineering practices • Identify software ID tagging as an Area for Future Improvement	• Improves the security, integrity and assurance of the technology deployed in an organization's environment
Focus the Framework's privacy guidance	• Align the Framework's privacy guidance with the scope of the Executive Order[3] • Focus on outcomes rather than prescriptive means	• Ensures that thoughtful, appropriate and implementable privacy guidance is put forth

[1] Federal Register Notice: "Request for Comments on the Preliminary Cybersecurity Framework", available at https://www.federalregister.gov/articles/2013/10/29/2013-25566/request-for-comments-on-the-preliminary-cybersecurity-framework.
[2] Response of Microsoft Corporation to Request for Information, available at http://csrc.nist.gov/cyberframework/rfi_comments/040713_microsoft.pdf.
[3] Executive Order 16363: Improving Critical Infrastructure Cybersecurity, §5, available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

	• Refrain from advancing broad, generally applicable privacy guidance • Identify evolving privacy concepts as an Area for Future Improvement	
Streamline the Framework's structure	• Integrate relevant security and privacy guidance in the Framework where activities intersect • Provide contextual definition for "adoption" of the Framework	• Encourages, and underscores the importance of, collaboration and alignment • Provides clarity to organizations and increases the likelihood of voluntary adoption
Allow an opportunity for public comment on the revised Framework	• Provide an interim release of the proposed final Framework	• Enables organizations to review important changes while evaluating adoption

Expand the Framework's security guidance related to secure engineering and asset management: In developing the final version of the Framework, NIST should broaden its discussion on secure engineering practices. Our basis for making this recommendation is that deployment of secure engineering practices could affect an organization's security posture by improving the security, integrity and assurance of the technology (hardware, software, services) deployed in an organization's environment. Secure engineering practices reduce the number and severity of vulnerabilities in deployed technology and establish appropriate processes to ensure maintenance and response, and improve resiliency of the systems designed with those tenants. Such practices have demonstrated a return on investment,[4] therefore, greater focus on secure engineering could help NIST achieve its intent to provide more cost-effective guidance.

NIST should also include software ID tagging, or SWID, as an area for future improvement in further iterations of the Framework. This emerging practice strengthens organizations'

[4] *See* Research Brief, Aberdeen Group, "Security and the Software Development Lifecycle: Secure at the Source," available at http://www.microsoft.com/en-ie/download/details.aspx?id=6968; and *See* Thought Leadership Paper, Forrester Consulting," State of Application Security: Immature Practices Fuel Inefficiencies, but Positive ROI Is Attainable", available at http://www.microsoft.com/en-us/download/details.aspx?id=2629.

awareness of their networks configurations and operating environments. It is bein piloted in government agencies, and critical infrastructure organizations may similarly benefit from application of this practice, particularly in their supply chain risk management effort.

Focus the Framework's privacy guidance: NIST should focus the scope of the Framework's privacy guidance to better align with the scope of the Executive Order's instructions to NIST regarding privacy in the Framework. The Executive Order directs incorporation of "privacy and civil liberties protections" that are "based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks."[5] The current privacy guidance goes beyond this mandate. Rather than focusing on mitigating specific privacy risks directly and uniquely implicated by an organization's cybersecurity practices or controls,[6] the Framework introduces a broad spectrum of provisions that ultimately prescribe implementation of a comprehensive privacy governance program based upon a very specific standard, NIST SP 800-53 Rev. 4 Appendix J. In its current form, the privacy guidance would create unnecessary, onerous compliance costs and risk discouraging organizational adoption of the Framework.[7]

Streamline the Framework's structure: There are two structural changes that NIST should consider for the final Framework. First, the division of security and privacy guidance into separate appendices in the Preliminary Framework encourages a siloed approach to security and privacy by implementing organizations. In practice, security professionals would look to Appendix A while privacy professionals would look to Appendix B, and potentially, never coordinate implementation efforts. Thus, NIST should integrate Appendices A and B into a unified Framework that is inclusive of both security and privacy guidance. This integration would create an opportunity for implementing organizations to consider privacy as an inherent element across all functions in the Cybersecurity Framework.

Second, there is a considerable amount of concern within the private sector about the absence of an articulated path for organizations' adoption of the Framework. Accordingly, NIST should define "adoption" in the Framework Glossary. Borrowing from language set forth in Appendix A of the Preliminary Framework, this definition should emphasize that

---

[5] Executive Order 16363: Improving Critical Infrastructure Cybersecurity, §5, available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[6] *See* Comments on the Preliminary Cybersecurity Framework, Hogan Lovells, available at http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf; and *See* Comments on the Preliminary Cybersecurity Framework, Hunton & Williams, available at http://csrc.nist.gov/cyberframework/framework_comments/20131213_fred_cate_huntonwilliams.pdf.

[7] *Id*.

organizations can adapt the Framework to support their risk management goals and needs. Absent a clear statement of what adoption means, a likely outcome is that the Department of Homeland Security's (DHS) emerging Voluntary Program would likely lack strategic direction from its foundational document, the Framework.

Allow an opportunity for public comment on the revised Framework: Much like the interim release for public comment on the Discussion Draft of the Preliminary Cybersecurity Framework, we recommend NIST strongly consider an interim release and comment period for the near-final Framework prior to its delivery in February. As the structure and content (particularly with respect to privacy) are likely to change significantly, an interim release would aid organizations who are working to determine whether and how to implement the Framework in their organizational policies, practices and procedures.

In conclusion, we again commend NIST on this milestone. We especially appreciate NIST's exceptional transparency and deep engagement with the private sector in the development of the Framework. We look forward to continued partnership with NIST and other government agencies on the Framework and related initiatives to strengthen the resiliency of critical infrastructure.

II. DISCUSSION

A. THE FRAMEWORK'S SECURITY GUIDANCE RELATED TO SECURE ENGINEERING AND ASSET MANAGEMENT SHOULD BE EXPANDED

The Framework Should Provide Broader Guidance on Secure Engineering Practices
NIST should broaden the Framework's guidance related to secure engineering practices, particularly given the importance of engineering to many critical infrastructure organizations. The Preliminary Framework provides only one line-item related to secure engineering, and its guidance is simply too light.[8] This guidance should be expanded to help organizations improve security of their hardware, software and services.

Specifically, we strongly encourage NIST to amend its current guidance to incorporate ISO/IEC 27034-1:2011 as an Informative Reference, and to provide guidance that is comparable to the following:

Category	Subcategory	Informative References

[8] NIST Preliminary Cybersecurity Framework, available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

Design and develop technology (e.g., hardware, software and services) in a manner consistent with international standards and industry best practices throughout the engineering lifecycle	• Utilize recognized secure development lifecycle process that includes guidance on relevant security and privacy practices, controls, and tooling across all phases of the engineering lifecycle (design, develop, review, test, approve)	• ISO/IEC 27034-1:2011

By providing this guidance, the Framework would focus attention on the importance of software assurance and sound organizational management practices. For software engineers, ISO/IEC 27034-1:2011 is specific and rigorous enough to address real world risk, and flexible enough to be broadly useable and meaningful to organizations. From an acquisition perspective, ISO/IEC 27034-1:2011 offers a concise internationally-recognized way to enable transparency into suppliers' software engineering management process.

Identify Software ID Tagging as an Area for Future Improvement

The Framework should identify software ID tagging, or SWID, as an Area for Future Improvement. Given the intent to have the Framework advance supply chain risk management, SWID is an important, developing practice to progressing guidance in this space. Specifically, ISO/IEC 19770-2 is an emerging standard that is supported by Microsoft and others in the industry, and enables developers and users to verify the origin of software. If a user organization understands which suppliers are implementing secure development practices in conformance with ISO 27034-1, application of ISO/IEC 19770-2 enables that organization to confirm that it is using software that came from those suppliers. Currently, NIST's National Cybersecurity Center of Excellence (NCCoE) and DHS are leading efforts to define the government's expectations regarding SWID. Accordingly, as these workstreams continue to develop and grow within the private sector and in government, they will be ripe for consideration and inclusion in future iterations of the Framework.

B. THE FRAMEWORK'S PRIVACY GUIDANCE SHOULD BE FOCUSED

NIST Should Revise the Framework's Privacy Guidance to Align with the Executive Order's Instructions

The Framework's privacy guidance exceeds the scope of the Executive Order, which states simply that agencies must "ensure that privacy and civil liberties protections are incorporated into" their activities under the Executive Order.[9] Instead, the Framework goes far beyond cybersecurity and imposes an overly prescriptive, comprehensive privacy governance program that all organizations would need to implement, across all functions, irrespective of size, scope and risk. For example, the Methodologies in the Governance Category would impose significant burdens on organizations as part of implementing a comprehensive privacy governance program, including addressing asset management and identification, access control, awareness and training, auditing and destruction. Even for mature organizations, implementing governance programs of this magnitude and specificity is costly and time consuming. By requiring a rigid, monolithic solution for all organizations, the Framework's privacy guidance not only goes far beyond the Executive Order, but may also discourage organizations from adopting the Framework.

Instead, the privacy guidance should focus on specifically targeting the unique privac impacts of cybersecurity activities.[10] In our attached comments sheet, we have identified specific instances where we recommend that the privacy guidance could be tailored to squarely address the privacy implications of certain cybersecurity activities. Through these recommendations, and those provided by other industry stakeholders,[11] the Framework could provide meaningful privacy guidance that is consistent with the Executive Order's instructions.

The Privacy Guidance Should Focus on Outcomes Rather than Prescriptive Means
The privacy guidance is overly-prescriptive and imposes a one-size-fits-all solution on all organizations, regardless of size, complexity and sophistication, and regardless of the sensitivity of the organization's activities related to privacy. Consequently, the privacy guidance could lead unnecessarily to onerous implementation burdens and unintended consequences, without actually addressing the privacy mandates from the Executive Order in a meaningful way.

For example, it may indeed be good practice for large organizations that maintain and share personal data under the Framework to understand the types of data in its systems. However, it may be unnecessary for other organizations that maintain and share only network data related to cyber incidents, to undergo the same comprehensive assessment

[9] Executive Order 16363: Improving Critical Infrastructure Cybersecurity, §5, available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[10] *See* Comments on the Preliminary Cybersecurity Framework, Hogan Lovells, available at http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.
[11] *Id* and Comments on the Preliminary Cybersecurity Framework, Hunton & Williams, available at http://csrc.nist.gov/cyberframework/framework_comments/20131213_fred_cate_huntonwilliams.pdf.

as suggested by the methodology in the Asset Management Category.[12] This type of prescriptive privacy guidance also risks falling out of date as technology, cyber threats and privacy practices continue to evolve. Instead, the privacy guidance should specifically target how to protect data associated with cybersecurity activities, as contemplated by the Executive Order. As was done with the cybersecurity guidance, the privacy guidance should similarly identify the desired outcomes and give the industry the discretion to develop the most innovative and appropriate means by which to achieve those outcomes.

Refrain From Advancing Broad, Generally Applicable Privacy Guidance

The Framework is not the appropriate vehicle for advancing broad, generally applicable privacy guidance. While avoiding overly prescriptive privacy guidance is important, so too is avoiding overly general privacy guidance that does not support or enhance specifi infrastructure protection efforts in the scope of the Executive Order. The current privacy guidance, while well-intentioned, could have broad-ranging implications far beyond cybersecurity. As we have seen in other instances where voluntary codes of conduct and best practices have been developed, voluntary frameworks often become the foundation for formal regulation and legislation. In addition, there are forums better suited to develop and propose broad privacy rules (e.g., Congress, the FTC); as demonstrated by various draft legislation and FTC enforcement actions. These entities with comprehensive experience in the privacy domain are better suited to develop broad, generally applicable privacy requirements.

Moreover, the privacy methodology has not received, and will not receive (as the privacy methodology is revised), the appropriate review and stakeholder input as compared to the cybersecurity guidance in the Framework. Only since the November Raleigh workshop has attention and feedback been given on the privacy methodology. More time for valuable consideration and input is necessary to ensure that thoughtful, appropriate and implementable privacy guidance is put forth in future revisions of the Framework.

Identify Evolving Privacy Concepts as an Area for Future Improvement

In addition to our line-item comments on the privacy guidance, we encourage NIST to be mindful of the evolving nature of privacy practices and frameworks in its discussion of Areas for Improvement. The Framework relies upon the Fair Information Practice Principles (FIPPs), but ignores any "other privacy and civil liberties policies, principles, and frameworks."[13] The Executive Order makes clear that by allowing for "other privacy and

[12] NIST Preliminary Cybersecurity Framework, Appendix B, pg. 28, available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[13] Executive Order 16363: Improving Critical Infrastructure Cybersecurity, §5, available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

civil liberties policies, principles, and frameworks", the privacy guidance does not have to be solely reliant upon the FIPPs. Rather, other privacy principles and frameworks could be utilized and we recommend such consideration.

The FIPPs is a principle based approach to privacy protection that was established over 40 years ago that is based largely on notice and individual consent. While the FIPPS were created in an era when notice and consent was more simple and meaningful, it is increasingly difficult to provide simple and meaningful notice and obtain truly informed consent. The realities of the data rich environment of the 21st century complicate and challenge the degree to which the FIPPs are effective.

The privacy community continues to debate the relevance of the current form of FIPPs and has sparked a debate around alternative frameworks, including those that focus on data use rather than data collection.[14] As subsequent iterations of the Framework are released and further meaningful thought is given to the intersection of privacy and cybersecurity, we encourage NIST to consider whether the historical FIPPs are the best foundation for privacy guidance of a cybersecurity Framework and to refrain from including them in the Framework until further dialogue can be had on this point.

C. STREAMLINE THE FRAMEWORK'S STRUCTURE

The Framework Should Integrate Security and Privacy Guidance in a Unified Manner
NIST should integrate Appendices A and B into a unified Framework that is inclusive of both security and privacy guidance. Our basis for this recommendation is that division of security and privacy guidance into separate appendices in the Preliminary Framework encourages a siloed approach to security and privacy by implementing organizations. This is likely to result in a fractured approach to mitigating risks of cybersecurity incidents and to managing the privacy implications of cybersecurity strategies.[15]

The Framework presents an important opportunity for privacy and cybersecurity professionals to collaborate towards the goal of improving their organizational cybersecurity posture.[16] These disciplines would work together to best understand how the Framework might apply to their organizations and how the Framework is to be implemented. Today, the unfortunate reality is that privacy and security professionals may

---

[14] *See* Fred H. Cate & Viktor Mayer-Schönberger, Data Use and Impact Global Workshop (2013), available at http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf; and *See* Fred H. Cate, Peter Cullen & Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century (2013), available at http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf.
[15] *See* Comments on the Preliminary Cybersecurity Framework, Hunton & Williams, available at http://csrc.nist.gov/cyberframework/framework_comments/20131213_fred_cate_huntonwilliams.pdf.
[16] *Id*.

have limited interaction with one another until required to do so, usually by a triggering event, such as a cybersecurity attack o data breach incident. That point in time may be too late for efficient and meaningful collaboration of privacy and security concerns in a unified manner.

To accomplish these objectives, we have shown in the line edits accompanying this filing, various touch points where there is an opportunity for meaningful collaboration among cybersecurity and privacy disciplines. For example, the Identify function could provide guidance that both privacy and cybersecurity roles and responsibilities should be identified, coordinated and aligned. In the Preliminary Framework, these roles are separated into different sections of the document and it is unclear how and to what extent these disciplines should develop practices in coordination with one another.

By integrating security and privacy guidance into a unified Framework, the Framework would encourage collaboration between security and privacy professionals through all stages of organizational implementation. Additionally, NIST would potentially reduce the overall cost of implementation because a unified Framework provides a single set of guidance, rather than the bifurcated approach presented in the Preliminary Framework.

Finally, a unified Framework would underscore the importance of systemic integration of security and privacy considerations. Such collaboration would enable organizations to leverage many of the ideas of Privacy by Design, which advances the view that technologies and systems should be developed in a manner whereby privacy considerations and impacts have been identified, assessed and mitigated from the outset and not addressed as an afterthought. There is a strong parallel between Privacy by Design and our recommendation above regarding the role of secure engineering practices.

Thus, we recommend incorporating the privacy activities specifically implicated by cybersecurity activities into the Framework rather than as a separate Appendix, to avoid the risks that are created by addressing privacy and cybersecurity in a siloed manner. With this shift, NIST might also lower the barrier to implementation for organizations that may not yet have a robust privacy program, without diminishing the Framework's functionality or flexibility.

The Framework Should Define Adoption

One of the key questions facing organizations is how to use the Framework, in particular, whether there is any difference between "implementation" as contemplated in the Framework Implementation Tiers and "adoption" as discussed in the Executive Order and DHS's forthcoming Voluntary Program. This ambiguity is unhelpful for both the private sector and the government; businesses lack clarity from the government about its expectations, thus the government's goals are frustrated. However, there is a simple solution that would help avoid this impasse.

The Framework should expressly define "adoption" to plainly explain that it means using the Framework as baseline guidance for cybersecurity activities and related privacy initiatives, with adaptation at the organization level to reflect organization-specific needs. Specifically, we recommend that the Framework define adoption as follows:

> **Adoption:** An organization (e.g., critical infrastructure owner or operator) utilizes the Framework as baseline guidance in its determination of appropriate cybersecurity risk management activities and related privacy protection efforts. This process should involve adaptation of the Framework to suit organizational needs, including identification of organization-specific activities that give effect to the goals of the Framework but may not be listed in the Framework. Where an organization has aligned its policies, practices, and procedures with an Informative Reference, or provided self-attestation or certification against an Informative Reference, the organization is operating at a fundamentally mature level of implementation.

Our basis, in part, for this definition is the Executive Order's instruction that the Framework be "flexible" in how it supports cybersecurity risk management.[17] Additionally, the Preliminary Framework explains that the Framework is intended to be fundamentally adaptable:[18]

> *[The Framework Core] is not exhaustive; it is extensible,* allowing organizations, sectors, and other entities to add Subcategories and Informative References that are relevant to them and enable them to more effectively manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional . . . [activities] may be added to the Profile. *An organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities . . . .*

This acknowledgement demonstrates that the Framework is not meant to be a prescriptive document that organizations must utilize in a flat manner. Instead, the Framework is fundamentally designed to offer different pathways to adoption based on organizational needs and requirements. For example, the Framework is unlike binary control sets prescribed by certain authorities because the security guidance in the Framework focuses on desired outcomes rather than specific controls that an organization must deploy.

---

[17] Executive Order 16363: Improving Critical Infrastructure Cybersecurity, §7, available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[18] NIST Preliminary Cybersecurity Framework, Appendix A, pg. 13, available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

We encourage NIST to provide clarity about how it intends organizations to utilize the Framework's guidance. By defining adoption, NIST would significantly improve organizations' ability to determine whether and how to use the Framework, and likewise, advance the government's goal of voluntary adoption. In the absence of such definition, it is likely that ambiguity surrounding the Framework's usage will persist, and robust voluntary adoption, as desired by government, may not occur.

D. NIST SHOULD PROVIDE AN INTERIM RELEASE OF THE PROPOSED FINAL FRAMEWORK

Based on public discourse surrounding the Preliminary Framework and particularly, its privacy guidance, we anticipate that NIST will make significant changes to at least some portions of the Framework. In that event, we strongly encourage NIST to provide an interim release of its proposed final version of the Framework prior to its February deadline. Our basis for this recommendation is that many organizations are working to determine whether they will adopt the Framework and participate in the forthcoming DHS Voluntary Program. By providing an interim review of the proposed final Framework, NIST would significantly aid these efforts in the private sector.

Additionally, as any effective cybersecurity framework must be a living document, providing an interim release enables NIST to gather further substantive input. Specifically, this would allow the privacy contributions to develop further, and NIST could, in later revisions of the Framework, bring privacy and security together more clearly where the two intersect, with the dependencies and connections between the two disciplines better mapped, and better understood. By focusing on future iterations of the Framework, NIST could create a more integrated core of key security and privacy priorities that are relevant for securing critical infrastructures in the United States. Thus, we recommend allowing more thoughtful consideration and development time to ensure that privacy does not remain a late addition to the drafting process.

III. CONCLUSION

Microsoft is committed to working with industry and government partners to help advance international standards and practices that enhance critical infrastructure cybersecurity. In addition, Microsoft remains willing to work with NIST and DHS on any of the comments provided here to help ensure the success of the Framework. Microsoft commends NIST for seeking industry input into developing a Framework, and looks forward to continued engagement with the government and our industry partners.