From: **Jessica Zucker (Wimmer Solutions Corporation)**
Date: Mon, Apr 10, 2017 at 5:01 PM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity - Microsoft Response
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: "Paul Nicholas", "Angela McKay", "Amanda Craig"

Dear Mr. Edwin Games,

Please find the attached response from Microsoft Corporation to the request for comments on the proposed update to the Framework for Improving Critical Infrastructure Cybersecurity.

Thank you for the opportunity to submit comments on the proposed Framework update. We look forward to following up and continuing the conversation around the feedback we have provided.

Best regards,

Jessica

--
Jessica Zucker
Cybersecurity Strategist | Global Security Strategy and Diplomacy
Corporate Legal & External Affairs | Microsoft
https://www.microsoft.com/en-us/cybersecurity/

[Attachment Copied Below]

Before the U.S. Department of Commerce
and the
National Institute for Standards and Technology

In the Matter of	)	
Proposed Update to the Framework for	)	
Improving Critical Infrastructure Cybersecurity	)	Document # 2017-01599

Response of
Microsoft Corporation
To Request for Information

Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
(425) 882-0808

April 10, 2017

Introduction

Microsoft welcomes the opportunity to provide comments to the National Institute of Standards and Technology (NIST) regarding the recently released Cybersecurity Framework Draft Version 1.1. 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, mature, share, and promote cybersecurity best practices both internally and externally.

We commend NIST's ongoing and iterative efforts to develop, implement, and refine the Cybersecurity Framework ("Framework"). Throughout the process, we have collaborated extensively with partners domestically and internationally, including industry, NIST, and other government stakeholders. Our efforts have centered on ensuring that the approach incorporates insights gained through experience and on promoting awareness and implementation of the Framework. We remain committed to working with industry and government stakeholders over the long-term to use, promote, and strengthen approaches that, like the Framework, are rooted in public-private partnerships, international standards, and best practices, helping to advance cybersecurity risk management globally.

Microsoft has also integrated the Framework into our enterprise risk management program to influence our security risk culture and inform how we communicate about security capability maturity across our senior management and with our Board of Directors. As an external best practice that applies across our key services and across different risk management roles, the Framework enables a conversation across practitioner and management teams with different expertise and different areas of focus. It also functions as one of several approaches our Enterprise Risk Management function uses to validate cybersecurity across the organization. For Microsoft, one of the key benefits is how the Framework establishes a common language, which we use to facilitate security maturity conversations across our offerings in a consistent way. Talking about security across our offerings in a consistent way simplifies communications for us, enabling senior leaders to actively engage in discussions about security activities and continuous improvements, including new investments in risk management processes or security capabilities.

In conversations with customers, partners, and other industry stakeholders, Microsoft has learned that our positive experience with the Framework is not unique. Indeed, since 2014, it has gained broad recognition as effective guidance for cybersecurity risk management. The Framework's broad applicability across sectors and organizations of different sizes has been critical to its success. Likewise, the Framework's flexibility enables organizations to assess cyber risks—in the context of broader enterprise risks and aligned their individual concerns, tolerance, and resources—and to augment the Framework's guidance as appropriate to address sector-specific or unique risks. In addition, the Framework's flexible approach and focus on enabling informed security investments over time supports continuous learning and improvement in the organizations that utilize it.

In today's complex environment, having a "baseline" (i.e., a set of foundational security best practices intended to manage common cybersecurity risks) that cuts horizontally across the different vertical sectors is essential because most organizations are dependent on and/or serving customers in other sectors. A cross-sectoral baseline is particularly helpful because it enables organizations to communicate with each other across sectors about risk management in a consistent manner, thereby driving improvements across a diverse ecosystem. In addition, as governments around the world develop,

update, and implement legislation, regulation, or guidelines to protect critical infrastructures, the Framework—as a cross-sector baseline to manage cybersecurity risks—can inform these national efforts and promote interoperability across jurisdictions. In an interconnected world, maintaining interoperability is essential not just for businesses to operate across countries, but also for governments' ability to collaborate on cybersecurity challenges, which most often cut across jurisdictional boundaries.

We offer the following high-level recommendations for improving Draft Version 1.1 and related efforts:

1. **Preserve and strengthen the Framework's broad usability** as a cross-sector baseline by ensuring that substantive updates are timely, relevant, and consistent with the current approach; and
2. **Significantly increase efforts to promote the Framework domestically and internationally** by positioning the Department of Commerce for a greater leadership role and ensuring that other Federal agencies prioritize and coordinate to foster greater awareness and use, including by moving relevant parts of the Framework to an international standards body.

We have provided more specific recommended action steps and accompanying analysis on these two themes in the subsequent sections: "Preserve and Strengthen the Framework's Broad Usability" and "Promote the Framework as a Global Best Practice."

1. Preserve and Strengthen the Framework's Broad Usability

The topical additions to Draft Version 1.1 reflect the security needs of a changing cybersecurity ecosystem. Updates to the Framework, however, must also be incorporated in a way that preserves and strengthens its usability. In particular, Microsoft identified three key areas of Draft Version 1.1 that should be reevaluated and revised consistent with that goal:

- Qualitative and quantitative approaches for understanding risk management posture and goals, including the measurement and metrics guidance, should be developed in supplementary documents rather than in the Framework itself. Ensuring a connection between cybersecurity risk management efforts and business outcomes is important, but approaches for doing so are not yet sufficiently stable nor adequately mature to include in the Framework. Furthermore, approaches may ultimately differ greatly across sectors, organizations of different sizes, and communities with different cybersecurity risk management objectives (e.g., availability versus confidentiality and integrity).
- Supply chain risk management should be integrated throughout the Core's Subcategories and Informative References rather than within the Implementation Tiers. Inclusion of supply chain security, a topical area, creates confusion about how to use of the Tiers; integration of supply chain security across relevant areas of the Core, however, more effectively incorporates all the organizational stakeholders whose responsibilities may contribute to overall supply chain security. In addition, the language on supply chain security throughout the Core should be simplified to ensure that it is applicable to and usable by the diverse community of Framework users. NIST should also update the Informative References to include international standards and best practices specific to supply chain security.

- To maintain relevance in a dynamic and evolving cybersecurity ecosystem, the existing language and updates in the Framework should continue to reflect an outcomes-based approach.

The Framework's core principles of bringing together risk-based, outcome-focused, prioritized, and practicable guidance, applicable across different sectors and organization sizes, is foundational to its broad usability. As further discussed below, we encourage NIST to continue to focus on these core principles in considering how new topics and guidance can be incorporated into not only this update but also to support the Framework ecosystem.

1.1 Develop measurements and metrics as supplemental guidance

Understanding cybersecurity risk management posture and goals in a way that is grounded in the context of an organization's business or mission is crucial. Moreover, finding a way to enable such understanding is an area of increasing interest and need for both governments and industry. For enterprises, recognizing this correlation between business objectives, cybersecurity risks, and efforts to improve risk management will help evolve risk management programs and promote greater executive awareness of and constructive engagement on cybersecurity. For governments, understanding the effectiveness of risk management investments across Federal departments and agencies is also important, as underscored in a recent Government Accountability Office report[1] to Congress. Going forward, both the public and private sectors need to ensure that growing interest and investment in cybersecurity policies and practices is used to help organizations achieve desired security outcomes and business objectives or other organizational missions.

While there is an increasing appetite for and a myriad of efforts underway to develop approaches to demonstrate the effectiveness of cybersecurity risk management activities and investments, in our experience and conversations with our industry partners and customers, these approaches are still relatively nascent and evolving. For example, Microsoft's approach to measuring penetration testing has changed over time. Previously we looked primarily at the number of successful attempted penetrations and the amount of time required to achieve that initial benchmark; now we also measure the path and techniques, tactics, and procedures (TTPs) used by testers to reach their actual target. This progression in measurements for penetration testing reflects an evolution of our thinking (to an assume breach mentality) and changes in network architecture and segmentation technology; it also helps ensure that investments focus on overall resilience. It helps us identify trends in TTPs and determine what combination of investments in mitigation techniques that protect, detect, contain, and respond to events will be most effective versus more narrowly and disproportionately focusing on protection.

In addition, conversations with partners and customers have revealed that they are also evolving approaches to assessing risk, the changing threat ecosystem, and the effectiveness of risk mitigation efforts. Like us, large and small businesses in every sector of the economy are working to develop, update, and refine approaches to assess and measure risk and the effectiveness of different mitigation techniques to hone their security investments and continuously improve their risk management posture.

---

1 http://www.gao.gov/assets/690/682756.pdf

Even once approaches to measurement are more stable, what different sectors and organizations measure, how they do so, and how they use that information to improve their efforts will likely vary significantly. Different sectors and organizations of different sizes will likely take different approaches to understanding cyber risks of concern, how they affect overall enterprise risk, and the respective roles and responsibilities of enterprises and governments in managing those risks to an acceptable level. More broadly, how organizations think about security also varies. For some, security is considered fundamental to an organization's business or mission viability; others view it as a cost of doing business. This difference in mindset results in considerable variability in how organizations approach understanding risk management posture and goals.

Recognizing that approaches to understanding organizational risk management posture and goals are crucial but still evolving and context dependent, we recommend that:

- The proposed Section 4 of the Framework be greatly streamlined; and
- Guidance on metrics and measurement be developed as supplementary and complementary documents to the Framework.

This approach would help to foster meaningful advancements. First, including a short, focused section that highlights the relationship between measurement and metrics and business outcomes would support ongoing organizational, sectoral, and other efforts to develop and mature a body of work on this topic. Second, developing supplementary guidance documents would ensure that the approaches that some users are finding to be effective are identified, documented, exchanged, and promulgated for greater use. Supplementary guidance will also enable multiple approaches to be articulated in support of sectors or other communities of interest, including those that face similar risks and challenges. For example, small businesses, which represent a significant community of interest, face similar risk challenges and demands for demonstrating return on investment. Supplementary guidance that is particularly responsive to the operational context and needs of small businesses is likely to be more useful to such organizations than a more conceptual discussion.

As NIST pursues efforts to develop supplementary guidance documents on metrics and measurements, we encourage continued focus on both qualitative and quantitative approaches as risk management posture and goals are informed by both. As part of those efforts, NIST should also revisit the definitions currently proposed in Draft Version 1.1 for "metrics" and "measurements" as, in our experiences both internally and externally, those labels both have quantitative connotations.

Qualitative approaches, which provide a foundation to assess risks, link security investments with business outcomes, and enable continuous improvement, are already incorporated within the Framework, but greater clarity on those could bolster implementation. For example, the processes associated with developing Current and Target Profiles and using the Implementation Tiers serve to help Framework users articulate their risk management posture and address gaps in meeting or exceeding their risk management goals. Rather than creating additional qualitative measurements, guidance in supplementary documents could clearly link guidance or use cases with these existing aspects of the Framework, which would encourage use of these approaches and better serve users' needs.

As an example of the kind of guidance that would be helpful, consider how organizations may use the Implementation Tiers in the context of different Categories and Subcategories. The Framework currently discusses assigning a single number to represent program, process, and external participation for each

assessment and Subcategory (as scoped). For a given scope, four different individuals with subject matter expertise could assign four different Tier ratings given the numerous subjective variables. In supplementary guidance, NIST could capture approaches that would help different subject matter experts engage to develop a shared understanding of "3." NIST could also highlight how the value of the Framework is using it as a tool to have such discussions. In addition, NIST could convey how maturity data can then be compared across a broader scope; more importantly, it can then provide a structure for senior leadership to define a target profile and for the evaluation of assessment data against the targets, informing strategic investments and planning.

Supplementary guidance on quantitative approaches is also needed and will require considerable work and deliberation. Quantitative approaches are very nascent, evolving, and context dependent, so NIST should consider convening groupings of different sectors or communities of interest or work within existing partnership forums, such as the sector coordinating councils, to develop use cases for metrics and measurement that ground approaches in examples and practical application. Moreover, NIST should ensure that guidance on quantitative approaches does not result in a focus on binary compliance, undermining the way in which qualitative guidance fosters continuous improvement. That key aspect of the Framework's value—fostering continuous improvements—results from the assessment process and internal conversations rather than the point-in-time Tier or maturity data.

Importantly, as supplementary guidance for both qualitative and quantitative approaches is developed, NIST and the community of stakeholders working on these efforts must ensure that they focus on how metrics and measurements are used to drive towards a purpose, lead to specific actions, and enable continuous improvement. An overemphasis on metrics and measurement without a clear linkage to purpose and use will result in a static, compliance-focused mindset and ultimately hinder overall culture and efforts to manage cybersecurity over time. In our experience, approaches that help organizations manage risks in a consistent, cross-company way and invest iteratively and dynamically over time are responsive to ever-changing circumstances and foster the necessary culture to drive continuous improvements in security and resilience.

1.2 Integrate supply chain security throughout the Core's risk management functions

Supply chain security is also a critical element of cybersecurity risk management and an issue of increasing concern. Today's information and communication technology products and services are derived from complex global supply chains, resulting in innovations, cost efficiencies, and distributed risks that impact both governments and industry. As a global technology provider with a diverse set of customers across a range of industries, Microsoft focuses on managing supply chain risks and responding to customer needs primarily in contractual requirements. In conversations with customers and partners, we've observed increasing awareness around the importance of managing operational dependencies, which will likely expand across sectors with different regulatory requirements and contractual preferences as the trend of "everything-as-a-service" continuously integrates a broader set of global, interdependent suppliers into more offerings.

As there is an increasing need and demand for organizations to manage supply chain risks and operational dependencies, NIST's inclusion of supply chain security in Draft Version 1.1 of the Framework is appropriate; however, we encourage NIST to reconsider *how* the topic is included—both

where the topic is included within the Framework and how baseline practices are positioned. More specifically, supply chain security should be:

- Integrated throughout the Core's Subcategories and Informative References rather than included within the Implementation Tiers;
- Simplified to ensure that it is applicable across the diverse community that uses the Framework; and
- Supported by Informative References that reflect international standards and best practices focused on supply chain risk management.

Supply chain security is a core commitment for Microsoft, and our approach and conversations with customers and partners inform our perspective on the importance of integrating supply chain security throughout the Core rather than including it within the Implementation Tiers. Our approach is multifaceted and, among many items, includes identity and access management, Security Development Lifecycle (SDL),[2] Operational Security Assurance (OSA),[3] software integrity policies and procedures, and anti-counterfeit measures. Our processes also continually evolve to incorporate new practices as we make new business investments, including in services. One of the key components of Microsoft's approach to supply chain risk management is that it does not live in only one component of our company but rather is integrated throughout the enterprise. Many different teams across various product and service groups contribute to supply chain risk management, including our antipiracy teams, hardware buyers, vendor program managers, and enterprise risk management group, which reflects the extent to which supply chain security is undertaken throughout the enterprise's overall risk management processes.

Since the Framework is cross-sector baseline with broad usability, how supply chain security is included in the context of the Framework should not necessarily reflect Microsoft's practices; however, a key takeaway from our own experience is that integration across the different parts of an organization is key in improving supply chain security. In addition, conversations with customers suggest that different business units or functions within and across sectors may manage various aspects of supply chain security or have different supply chain risk management priorities. Growth of "everything-as-a-service" will further complicate supply chains, and subsequently increases the importance of an integrated, cross-organizational approach to supply chain risk management.

Microsoft's experiences with using the Framework also indicate that incorporating supply chain security within the Implementation Tiers will not only limit risk management impact but also cause confusion. Prior to Draft Version 1.1, criteria within the Implementation Tiers have focused on attributes of maturity that cut across topics, rather than including specific topical or domain areas; the topic and domain areas have instead been built into the Core. As we have advocated for in previous feedback to NIST on the Framework,[4] greater clarity around the distinctions between adjacent Implementation Tiers would increase usability. However, adding any topical area to the Implementation Tiers obfuscates

---

[2] https://www.microsoft.com/en-us/sdl/

[3] https://www.microsoft.com/en-us/SDL/OperationalSecurityAssurance/

[4] Federal Register Notice Views on the Framework for Improving Critical Infrastructure Cybersecurity – 2015: https://www.nist.gov/sites/default/files/documents/2017/02/14/20160223_microsoft.pdf; 2014: http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf; 2013: http://csrc.nist.gov/cyberframework/rfi_comments/040713_microsoft.pdf

organizations' differentiation between Tiers, necessitating further subjective judgements about whether and how to include Tier criteria in assessments.

In addition to integrating supply chain security, a topical area, throughout the Core, NIST should ensure that practices are sufficiently simplified to be applicable across the diverse community that uses the Framework; greater detail, which may be applicable to some stakeholders, should then be included in supply chain security-focused references. In terms of structure, rather than creating a new supply chain Category within a particular Function, supply chain security should be integrated within relevant Subcategories and Informative References across different Functions. In terms of substance, NIST should focus on including baseline practices, such as software assurance and secure development practices, that are applicable to the broad array of organizations that now develop their own software. Greater details on these topics and other supply chain risk management guidance should then be included as supply chain-focused Informative References. For example, NIST should more substantially leverage existing international standards, including ISO 27036 and ISO 27034, as well as relevant best practices, including NIST SP 800-161, as Informative References.

1.3 Foster agility and resilience through an adaptive, outcomes-focused approach

In today's technology environment, an adaptive, outcomes-focused approach to cybersecurity risk management is critical, not only to ensuring continuity and continuous learning but also to enabling integration of the latest technologies and security capabilities. Both the threat landscape and technology products and services are rapidly evolving; offensive capabilities are constantly advancing, and technologies such as cloud, the Internet of Things, and software-defined networks are creating new security challenges and opportunities. To keep pace with the rate of change and take advantage of new services and features, defensive capabilities must constantly evolve and advance.

Considering this context, the Framework should both continue to use an adaptive, outcomes-focused approach to the greatest extent practicable and continue to incorporate international standards to enable compliance agility. Focusing on outcomes enables stakeholders to respond to the ever-changing threat environment and take advantage of new services, features, and defensive capabilities while using consistent risk management language. Moreover, by continuing to use an adaptive, outcomes-focused approach in the Framework, NIST will ensure continuity and help organizations recognize the need to continuously adapt defensive measures and focus on resilience. International standards can also be leveraged as a tool for improving resiliency and agility in the evolving cybersecurity ecosystem. Such standards are relatively stable and can anchor the Framework in demonstrating reciprocity across different certifications and compliance regimes.

Since the NIST Cybersecurity Framework provides useful, outcomes-focused guidance for improving cybersecurity risk management, its application in the context of newer technologies, including cloud computing and IoT, should also be highlighted. Around the world, public and private sector cloud adoption is on the rise, driven by the desire to harness the enormous potential for innovation, efficiency, security, and resilience. As cloud enables greater access to ICT resources, it also powers new industries that have not traditionally needed to incorporate cybersecurity into their products and services; many of these companies, which are now developing software, do not yet understand how to manage cybersecurity risks, even as their Internet-enabled devices continue to proliferate into virtually

every market. In this context of rapid change and new security opportunities and risks, the Framework can serve as a baseline tool, provide effective operational risk management practices relevant across sectors or technology areas. In addition, as with any particular sector or technology area, cloud or IoT providers may benefit from partnering with NIST or other stakeholders to develop guidance around how the Framework can be used in their particular context and what unique considerations may arise in doing so.

Recommendation 1: Preserve and strengthen the Framework's broad usability

Action Steps:

a) **Develop supplementary guidance for metrics and measurements** to foster understanding of cybersecurity risk management posture and goals;
b) **Integrate cyber supply chain risk management into the Core's Subcategories and Informative References**, embedding simplified, baseline practices and supply chain security-focused standards and removing the topic from the Implementation Tiers; and
c) **Update the language and terminology throughout the Framework** to reflect a threat landscape that will evolve over time[5] (i.e. changing "back-ups" to "creating resiliency").

2. Promote the Framework as a Global Best Practice

Microsoft not only uses the Framework internally[6] but also promotes it as a best practice both domestically and internationally; our experience and interactions with customers and partners have demonstrated that the Framework is an effective approach to cybersecurity risk management. The Framework helps to structure discussions to advance risk management processes and determine investment priorities. Importantly, the Framework 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 and investment.

From our engagements with governments and customers around the world, interest in cybersecurity and appetite for good approaches is strong and growing. Government stakeholders in particular are deeply concerned about cyber risks, and eager to move forward to demonstrate commitment to, leadership on, and progress on this strategic and operational challenge.

On a positive note, the Framework is often raised by stakeholders as one approach to consider. However, there are significant gaps in awareness, of the Framework itself and in understanding *why* the Framework is effective and *how* it was developed and has evolved. More specifically, in Microsoft's public policy work with governments and conversations with industry, we have learned that there is an interest in understanding how NIST convened diverse stakeholders; how NIST managed the process of

[5] Microsoft has provided specific examples and line edits in the appendix.
[6] http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf
http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160223_Microsoft.pdf

developing and evolving the Framework in a way that met the needs of different stakeholders; what the strengths of the Framework are; and why a cross-sectoral outcomes-focused approach is important in improving cybersecurity risk management.

There is not only an opportunity for but rather a need for the U.S. Government to promote the Framework, the approach used to develop it, and the attributes that make it effective—both domestically and internationally. Use of the Framework will help to enhance cybersecurity in the United States and beyond and, importantly, will advance U.S. economic and national security interests as well. In particular, Microsoft identified three primary objectives—two focused internationally and one domestically—that the U.S. Government should act on:

- U.S. economic and national security interests are directly affected by cybersecurity domestically and abroad. As such, the U.S. Government, led by the Department of Commerce, supported by the White House, and in coordination and collaboration with the Department of State and Department of Homeland Security (DHS), should promote the Framework and Framework-like approaches globally as the keystone economic objective of this Administration's international strategy and engagements on cyber.
- While some agencies and staff seem to recognize the strategic opportunity, and need, to promote the Framework internationally, doing so is not consistently prioritized relative to individual agencies' programmatic efforts or synchronized across agencies. Efforts to promote the Framework internationally should be prioritized, consistent with their importance to the U.S. economy and security, and coordinated across agencies and the opportunities afforded by their missions. More specifically:
    - NIST should move relevant parts of the Framework into an international standards body and collaborate with the State Department and DHS to enable their efforts; and
    - The State Department should undertake a set of activities to raise awareness of and promote the Framework in bilateral engagements, as well as regional and multilateral forums.
- Many U.S.-based organizations, including government agencies and the private sector, are familiar with the Framework. However, there is still an opportunity for broader promotion of the Framework and continued support for its implementation across sectors and communities of interest. In particular, use of the Framework by Federal agencies and U.S. critical infrastructure organizations should be a strategic priority, and DHS should highlight the value of the Framework for critical infrastructure protection.

2.1 Champion the Framework, and Framework-like approaches, as the keystone economic objective within U.S. international strategies and engagements on cyber

Internationalization of effective approaches to cybersecurity risk management, such as the Framework, is essential, not only to improving the overall security of the ecosystem but also to advancing the economic interests of the United States.

The security benefits of promoting the Framework are clear and would have a meaningful effect in the relatively near team. Improving the cybersecurity of companies around the world directly impacts U.S. national security interests because the U.S. Government and critical infrastructures are dependent on

global supply chains. As noted earlier, the horizontal integration of global supply chains across sectors and across regions creates considerable benefits, including lowering costs and promoting innovation and choice, but it also creates a source of risks that should be managed. If other governments and companies around the world use the Framework, then the overall cybersecurity of organizations in the supply chain will be improved, positively impacting security in the United States.

The economic benefits of promoting the Framework, on the other hand, are equally strong but perhaps not as immediately obvious. The economic implications are the result of risk management and business practices that U.S. businesses adopt or are required to adopt to access international markets. More specifically, companies must comply with national and sometimes regional requirements for security, but without widely referenced policy guidelines that governments are consistently leveraging, many are reinventing the wheel. This duplication and fragmentation of security requirements creates new compliance regimes that increase costs, often with minimal positive or even negative impacts on security. Microsoft is tracking more than 80 countries that are in the process of creating new cybersecurity legislation and regulations, and a myriad of implementing requirements are being considered. To the extent that these countries leverage, build from, and further develop the Framework and/or similar approaches with demonstrated results, the compliance, engineering, and operating costs for U.S.-based companies operating abroad would be lowered, supporting U.S. economic growth. Moreover, as greater horizontal integration is an ongoing trend, increasingly impacting not just ICT providers but also other industries, including energy and financial services, the extent to which globally aligned, cross-sectoral approaches will impact U.S. economic interests will also intensify.

Promoting the Framework globally should be the keystone of the economic objective of this Administration's international efforts for cyberspace because of the significant growth in and economic implications of regulatory fragmentation globally. The overall strategy and accountability for this effort should be led by the Department of Commerce, from the Secretary's office, and with roles for not only NIST, but also the International Trade Administration (ITA).

The Department of Commerce, including NIST and ITA staff, and working with industry partners, should develop core positions to discuss with their peer communities. The challenges that fragmented security requirements create for market access, the competitiveness of industry, and innovation, and, even more importantly, the benefits of interoperability to other countries' economies and security should be highlighted in bilateral, multi-lateral, and regional trade missions and negotiations, with a nearer-term focus on markets where regulatory efforts affecting critical infrastructures and/or digital service providers are underway (e.g., the European Union, Singapore) and where there is considerable interest in the Framework (e.g., Japan). Such strategic investments should be supported by the White House to ensure that the goals and benefits are appropriately connected to and synchronized across portfolios that have a cyber component (i.e., the National Economic Council and the National Security Council) and to ensure interagency coordination necessary to realize this goal is managed. Such investments should also be complemented and supported by the agency-specific work detailed in the following section.

When considering if and how to advance this recommendation, we urge the U.S. Government to consider the risks of inaction. The costs to the nation—in terms of economic and security impacts—would be very high. For the government, lack of investment now will result in increased costs in the future as managing fragmented regulatory requirements are resource intensive, requiring extensive personnel, expertise, and time to negotiate approaches that bridge regimes. For example, reconciling privacy requirements with Europe has created considerable costs. Fragmented security baselines will

also limit the diversity of compliant technology and security providers available to serve U.S. Government departments and agencies, limiting choice and increasing costs.

Finally, security benefits that could accrue to the interests of the United States will be at best delayed, and more likely significantly reduced, as both U.S.-based and international companies redirect resources from security to compliance with fragmented requirements. Moreover, the invaluable ability to exchange best practices with other organizations and determine what works based on common approaches, especially in early security baselines development stages, will be forfeited.

For industry, as noted above, fragmented security baselines divert resources toward compliance over security and risk management, driving up costs and limiting security improvements. In fact, the costs are multiplied, as differing prescriptive requirements lead to additional engineering of systems, audits conducted in different ways, and modifications to manage a continuous flow of policy changes. This also limits security innovation, as resources and expertise focus on static compliance, which does not provide sufficient flexibility to enable new techniques, capabilities, and architectures that could be developed and deployed. The cost of investing in or leveraging resources across borders will also increase, constraining the global innovation and manufacturing relationships that have helped to not only increase global economic opportunity but also drive down the costs of developing and popularizing advanced technologies.

Ultimately, the potential economic and security benefits of action and the risk of inaction justify a more strategic investment across the U.S. Government. The Commerce Department, in particular, is well positioned to advance national economic interests related to cybersecurity. To empower it to do so, we recommend that:

- The Department of Commerce is appropriately resourced and held accountable for promoting the Framework as the keystone economic objective of this Administration's international efforts for cyberspace; and
- The Department of Commerce and the White House include harmonization of cybersecurity requirements in bi-lateral, multi-lateral and regional trade and security missions and negotiations.

2.2 Enhance individual U.S. Government agencies' approaches to internationalization

Consistent with recommendations Microsoft has previously made, we continue to advocate for and stress the importance of action by various specific U.S. Government agencies to promote the Framework and the public-private partnership model that led to the Framework's development. Across the globe, there are numerous ongoing and important conversations, including on how to secure critical infrastructures, improve operational risk management, and respond to incidents, in which a more coherent approach to diplomacy, direct engagement, and supportive efforts by NIST, the Department of State, and DHS would be impactful. The lack of clear, shared cross-governmental objectives for cyber, echoed and supported by individual agencies based on their mission, authorities, and expertise, has driven inconsistency and reduced the effectiveness of U.S. Government engagements in these important global conversations.

This incoherence and a tendency to speak about the situation in the United States rather than about the broader context, challenges, and policy landscape relevant to others is contributing to the trend of countries moving past U.S. approaches. This directly contributes to the weakening of the global

cybersecurity ecosystem, creates political and regulatory challenges, and hurts businesses that operate across jurisdictions—as discussed in the previous section. The inability of the Government of 20 (G20) to collectively advance a draft cybersecurity norm in recent negotiations, purportedly due to U.S. concerns, is demonstrative of this issue; the decision not to advance this norm, through which governments would have agreed to refrain from tampering with or degrading the integrity of financial services data, was a missed opportunity from a risk management perspective, and therefore extremely disappointing to Microsoft and to the international financial community. It also highlights the need for the White House to play a stronger leadership role, ensuring strong private sector engagement and the consideration of both economic and security priorities. With strategic support from the White House, NIST, the State Department, and DHS should also exercise specific roles that reflect a cohesive U.S Government position.

2.2.1 NIST should drive standardization and support other agency efforts

Because the Framework's viability as a global reference point may be hindered in some contexts by a national government label, a vital step in internationalizing the Framework is moving some components or aspects of it into an international standards body. As Microsoft has advocated for in the past, aspects of the Framework will likely continue to benefit from being updated and governed by NIST. However, we encourage NIST to immediately begin working to transfer relevant aspects of the Framework to an international standards group. In particular, the Framework's Core is most relevant for standardization, and NIST should consider which aspects of the Core will be most stable over time and thus relevant for inclusion within an international standard. NIST should also promote internationalization with standards peers in other governments. Moreover, as NIST moves forward with this effort, a focus on synchronization of the Framework and any international standards efforts must be prioritized.

In addition, as part of its overall leadership on the Framework, NIST, with State Department and DHS participation, should also host a specific workshop focused on international considerations, challenges, and priorities. The workshop would solicit greater input on internationalization and direction to shape NIST's efforts and help other agencies understand the Framework and industry's interests, informing their efforts going forward. Moreover, NIST and its partners across the U.S. Government can exercise leadership in demonstrating the connection between the Framework and the growth internationally of critical infrastructure protection policies. As a globally respected government and industry partner, NIST's promotion of the Framework will support implementation in the United States and beyond.

2.2.2 The State Department should enhance strategic engagements in partnership with NIST

The State Department's Office of the Coordinator for Cyber Issues is uniquely positioned to be able to leverage its role in global cyber diplomacy to promote use and drive awareness, an activity which is consistent and aligned with one of its core missions: cybersecurity capacity building. However, to fulfill this mission, NIST must help build the State Department's own capacity on this subject and be a strategic partner. As a starting point, the State Department should:

- Translate the Framework into at least the six official languages of the United Nations;
- Partner with NIST to develop and translate guidance around the public-private partnership model that led to the Framework's development;

- • Partner with NIST to train diplomats—in particular, by hosting training on the Framework and public-private partnerships for diplomats going through the Foreign Service Institute. The State Department's annual Digital Economy Officers (DEO) Training Program would be an ideal starting point for collaboration to enhance DEO training on Internet and telecommunications policy;
- Include the Framework as an important priority in its bilateral discussions on economic advancement, security, and capacity building; and
- Host workshops, in partnership with NIST, in key capitals and regions overseas with foreign government representatives interested in learning about public-private partnerships, the Framework, and what makes the Framework an effective approach to cybersecurity risk management.
- A close and continuous partnership between the State Department and NIST is crucial in leveraging the U.S. Government's depth of expertise in cyber risk management and breadth of resources and diplomatic context.

2.2.3 DHS should foster use of the Framework in partnership with NIST

Use of the Framework internationally is important, and it is best supported by use domestically—both by industry and by government. Domestic use of the Framework will result in security and economic benefits in the U.S. akin to those that international use will result in on a global scale, improving ecosystem-wide approaches to cybersecurity risk management and limiting regulatory fragmentation amidst increasing horizontal integration of sectors.

As part of its mission to improve cybersecurity and critical infrastructure security, DHS should foster and support use of the Framework in both the public and private sectors. One of DHS's core areas of focus is protecting Federal networks,[7] and as a result of that mandate, DHS is well positioned to advocate for the adoption and use of cross-government approaches that would advance cybersecurity risk management and operational security. Consistent with its mandate and cybersecurity leadership position with the U.S. Government, DHS could also implement the Framework to secure its own operations, sharing lessons learned in doing so with other agencies.

Another core area of focus for DHS is the protection of critical infrastructure, and as such, it maintains a leading role in coordinating not only with Federal but also with state and local agencies as well as private sector partners.[8] DHS can enhance its role in both broadening stakeholder awareness of and supporting implementation of the Framework by developing sector-specific use cases, hosting workshops in coordination with state or local governments and industry partners, and developing training resources or supplemental guidance that's responsive to issues raised in such forums.

Given a mission space that cuts across the public and private sectors, DHS is also well positioned to highlight the cascading impacts of government adoption of the Framework on the broader ecosystem, including on critical infrastructure protection. To the extent that U.S. government organizations utilize the Framework for their own cybersecurity risk management programs and in their procurement

7 https://www.dhs.gov/topic/securing-federal-networks
8 https://www.dhs.gov/topic/critical-infrastructure-security

policies, they will not only better manage their organizational risks but also drive adoption of existing best practices, both with their direct and indirect suppliers.

Recommendation 2: Promote the Framework as a global best practice

Action Steps:

1. **Prioritize Framework promotion globally** as the keystone of the economic advancement portion of this Administration's international strategy for cyberspace, positioning the Department of Commerce to lead, in coordination with the White House, a cohesive cross-agency strategy;
2. **Pursue international standardization of the Framework**, including relevant parts of the Core;
3. **Drive global awareness and use of the Framework, as well as NIST's approach to public-private partnership**, through NIST, Commerce Department, State Department, and DHS efforts and engagements; and
4. **Continue to foster awareness and use of the Framework**, not only with industry but also across both Federal and State departments agencies, through DHS efforts and advocacy.

Conclusion

The Framework continues to be a meaningful part of Microsoft's enterprise risk management program, and we thank you for the opportunity to continue to contribute to its development. While topical updates to the Framework, when and where appropriate, are critical to responding to the evolving cybersecurity ecosystem, NIST should maintain focus on the Framework's broad usability. Moreover, as the Framework evolves, enabling agility and focusing on resilience in a changing ecosystem will ensure that the Framework remains relevant. Meanwhile, much more must be done in promoting the Framework's adoption in the United States and beyond. Internationalization will strengthen the U.S. economy and national security, consistent with this Administration's stated priorities. In closing, we welcome the opportunity to continue the conversation prompted by this RFI with NIST and other stakeholders.

Sincerely,

J. Paul Nicholas
Senior Director, Global Security Strategy and Diplomacy
Microsoft Corporate, External & Legal Affairs

Appendix A: Microsoft responses to RFI Questions:

RFI Question	**Microsoft Response**
Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?	Yes, see below line-edits and attached cover letter.
How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?	See the attached cover letter.
For those using Version 1.0 already, would the proposed changes impact your current use of the Framework? If so, how?	Yes, see attached cover letter.
For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?	N/A
Does this proposed update adequately reflect advances made in the Roadmap areas? Is there a better label than "version 1.1" for this update?	NIST expanded the language in the Access Control Category, consistent with the Roadmap's Authentication themes. Version 1.1 is an appropriate label for this update. In promoting international awareness of the Framework and NIST's approach to public-private partnership, U.S. Government agencies and NIST should demonstrate the significant continuity between Version 1.0 and Version 1.1.
Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?	We suggest that metrics and measurements be included as a topic in the Roadmap; specifically, the Roadmap could describe NIST's intention to convene stakeholders to develop multiple metrics and measurements-focused documents, including guidance and use cases, which would ultimately be supportive of rather than included within the Framework.

Appendix B: Microsoft line-edits to NIST Cybersecurity Draft v. 1.1

Section	Current Language	Microsoft's Feedback
Framework Core (all)	N/A	Baseline cyber supply chain risk management best practices, including software assurance, and ISO/IEC 0243, ISO 27036, NIST SP 161, and "Purchasing secure ICT products and services: a buyer's guide" (an EWI publication) should be integrated throughout the Core's Subcategories and Informative References, embedding supply chain security across responsibilities and at each stage of an organization's risk management process.
Risk Assessment: ID.RA	ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources	"Or any other external source" should be added after "informing sharing forums," more clearly scoping in security researchers or accidental vulnerability finders. In addition, ISO 29147 and ISO 30111 should be included as Informative References because they describe processes for receiving vulnerability information from third party finders, communicating with finders about reported issues, and investigating, triaging, and resolving vulnerabilities, all of which are in line with the sub-category objective of receiving vulnerability information. Alternatively or additionally, NIST could add a subcategory to Risk Assessment (ID.RA) – "*ID.RA-7: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from external sources*" – and cite ISO/IEC 30111:2013 and ISO/IEC 29147:2014 as Informative References. In conjunction with these efforts, NIST could also assess how to make clear that coordination with external researchers or vulnerability finders, as well as maturity in operationalizing information received from external sources, are included within the scope of the External Participation property of the Implementation Tiers. However, consistent with our recommendation on cyber supply chain risk management, we do not recommend that the Tiers became a landing space for narrowly focused, topic-specific guidance around levels of investment in relevant risk management activities. Rather, relevant maturity guidance may be included as an Informative Reference, providing a resource for internal conversations around investments and maturity.

Section	Current Language	Microsoft's Feedback
Protect: Identity Management, Authentication and Access Control Protect: Identity	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege, separation of duties, and high confidence methods of authentication where appropriate in terms of risk. Also include SP 800-63-3 as an additional informative reference. Consider including relevant FIDO standards.
Management, Authentication and Access Control	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate and in accordance with risk management principles.
Protect: Data Security	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	PR.DS-6: Processes used to verify the software, firmware and information integrity are in place.
Protect: Data Security	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	PR.DS-8: Processes are in place to verify hardware integrity that are focused on protecting and improving hardware security NIST 800.147 should be included as an informal reference.
Protect: Information Protection Policies and Procedures	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	PR.IP-4: Information redundancy (or resiliency) is implemented, maintained and tested periodically.